

## Visa/Dankort Rules

### 1. Introduction

These Visa/Dankort Rules apply to the use of Visa/Dankort in Denmark and abroad. The Visa/Dankort Rules apply irrespective of whether the card is used for payment in physical stores or for online purchases.

They apply to Visa/Dankort as physical cards and as cards in a wallet.

A glossary of terms can be found in section 23.

### 2. What can you use Visa/Dankort for?

Visa/Dankort is a payment instrument that you can use in Denmark and abroad, wherever the card is accepted.

If a store accepts both Dankort and Visa, it may have selected Dankort or Visa as its preferred payment method. In accordance with applicable legislation, the store must ensure that you can change this choice and pay with the part of the card you prefer. This can be done via the payment terminal.

Your account statement will always state whether a payment has been made as a Dankort or Visa transaction.

Please note that you may incur fees when you pay with Visa abroad, and that the monthly spending limit on your Visa card is written down by the transaction amount – even if you pay using the Visa part of your Visa/Dankort in Denmark, cf. section 2.4.

#### 2.1 Cash withdrawals

You can use either Dankort or Visa to withdraw cash from ATMs that accept Dankort and/or Visa. You can also use Dankort to make cashier withdrawals from your own and most other Danish banks, and you can use Visa in banks that accept Visa.

Please note that not all Danish ATMs accept Dankort cards. In such cases, the withdrawal will take place as a Visa withdrawal, and a fee may be charged for the withdrawal. The fee calculated by your bank is stated in the price list.

#### 2.2 Purchases in stores

You can use Visa/Dankort to pay for goods and services in stores that accept Dankort and/or Visa. You can also use your card for online purchases, as well as mail orders and phone orders. You can furthermore use Visa/Dankort for payment in self-service vending machines.

A sign displayed in the store or on its website will indicate whether Dankort and/or Visa are accepted.

If an amount has been credited to you by a store, the store may be able to deposit the money in your account via your Visa/Dankort.

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

For purchases abroad using a Visa card, you may be asked to choose whether the purchase is to be made in local currency or Danish kroner. See more details in section 18.4.

#### 2.3 Withdrawal of amounts from your account

As a general rule, purchases and withdrawals (transactions) using your Dankort will be deducted from your account on the same day as you use the card. Visa transactions will not be shown until the day after the purchase or withdrawal.

#### 2.4 Spending limit

You can only withdraw in cash or spend the amount held in your account, unless you have agreed otherwise with your bank – see sections 2.6-2.10.

#### 2.5 Contactless function or card in a wallet

If you use the contactless function or card in a wallet (e.g. Dankort on mobile), there is an amount limit that determines whether you need to enter a PIN code. You can see the 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 applicable payment limit, you will automatically be asked to approve the payment by entering your PIN code. On some occasions, you may be asked to enter your PIN code, even if the amount is within the applicable limit.

#### 2.6 Gambling and lotteries

When a Visa/Dankort card is used in stores that mainly offer gambling and betting, including casinos, lottery ticket dealers, racecourses and similar venues, a maximum amount per 24 hours may be set. The maximum amount is stated in the price list.

## 2.7 Withdrawals

Visa/Dankort has a maximum withdrawal amount per day. The amount is stated in the price list.

## 2.8 Visa – maximum amounts

Visa has a total maximum purchase and withdrawal amount per 30-day period. Within the total maximum amount, there are limits to the amount of cash per day you can withdraw using a Visa card from banks and ATMs. The amounts are stated in the price list.

## 2.9 Other conditions

Each store may set restrictions for the use of the card.

There may be a limit to the amount you can withdraw from banks and vending machines. You may be charged a fee whenever you withdraw cash, irrespective of the amount.

## 2.10 Card in a wallet with limited right of withdrawal

You may allow other parties – e.g. your child – to use a virtual card in a wallet (e.g. Dankort on mobile) to pay using your Visa/Dankort, subject to special restrictions.

This can be done via special mobile phone apps, where you create a payment option via your Visa/Dankort and set limits on the payment amount. Once set up, the person can pay in stores using his or her mobile phone.

Registration and user instructions for the function will be shown in the app.

## 2.11 Loyalty programmes

You can link Dankort and Visa to various loyalty programmes.

A Dankort may only be linked to loyalty programmes approved by Nets. You can see which programmes have been approved here <http://dankort.dk/Pages/Loyalitetskort.aspx>.

## 3. Use of Visa/Dankort

### 3.1 Payment

Before approving a payment or withdrawal, always check that the amount is correct. Payments that you have approved cannot be revoked. See sections 8 and 9, however, concerning reimbursement of a payment.

As far as possible, you should always obtain a receipt for your transaction (although in certain self-service vending machines you will not receive a receipt). Always check that the amount matches the purchase or payment, and that the date is correct. Always save the receipt until you have checked that the correct amount has been drawn from your account, cf. section 7.

Your Visa/Dankort can be used for payment in the following ways:

1. Reading/checking data from the card via
  - Chip or magnetic stripe and PIN code
  - Chip or magnetic stripe and signature
  - Contactless function
  - Wallet – e.g. Dankort on mobile
  - Chip or magnetic stripe in self-service vending machines without a PIN code
2. Entering details from the card (e.g. when making online purchases where data is not read electronically)
  - Registration of card number, expiry date and security code (typically when you enter information yourself)
3. Pre-registration of card details, e.g.
  - Agreement with an individual store to register card details, so that you can make future purchases approved and created by you.
  - Subscription whereby the store itself draws amounts by specific agreement with you.
  - Agreement with a digital wallet provider, whereby you register your card details for future purchases approved and created by you.

When you enter your PIN code, always make sure that no one else can read your code.

Never sign a transaction receipt if the amount has not been added or if the amount is incorrect.

If you become aware that several prints of the card are being made, you should always ensure that any unused prints are destroyed.

If you allow the store to draw extra money on your Visa/Dankort, e.g. as tips, always make sure that the store provides a receipt for the full amount.

When you use Visa/Dankort for e.g. car hire or during check-in at a hotel, it is customary for you to be asked to allow the car hire company or hotel to subsequently deduct additional amounts. Please note that the car hire company or hotel will then be able to subsequently draw on your account (see section 8).

Car hire companies and hotels may also reserve an amount via your card to cover all or part of the final bill. However, a store may only reserve the amount for which you have given consent.

### 3.2 Contactless function

If your card has contactless functionality, you can opt to use the contactless function when you shop in stores which offer this service.

In terminals where the contactless function is available, you can use the card without inserting it into the terminal. Instead, you accept payment by holding the card close to the terminal (distance of 0-3 cm). The contactless function is indicated by the following symbol on the terminal:



There is a limit to the amount that can be paid for each transaction without you having to enter your PIN code, cf. section 2.5. On some occasions, you may be asked to approve a payment by entering your PIN code, even if the amount is within the applicable limit for purchases using the contactless function.

### 3.3 Dankort on mobile and cards in wallets

You can link your Visa/Dankort to an app on your mobile phone and pay e.g. using your Dankort via this function (Dankort on mobile). You can see a list of approved wallets on Dankort's website – <http://dankort.dk/Pages/Dankort-i-apps.aspx>. You can register your Dankort card in all approved wallets that allow Dankort on mobile from your bank. Registration takes place using NemID (or similar security). Register the physical card you wish to pay with in the app. You will also be asked to select a personal PIN code that you must use if a purchase e.g. using Dankort on mobile requires you to enter a PIN code.

Information and instructions for set-up and use will be shown for the selected wallet. Your bank may set a limit for how many times you can connect a physical Dankort to your mobile phone.

You cannot use Dankort on mobile to shop online or for mail orders and phone orders.

### 3.4 Self-service vending machines without a PIN code

In some self-service vending machines, you can use Visa/Dankort without entering a PIN code or using a signature. In such machines, you accept the transaction when your Visa/Dankort is read by the vending machine or when you subsequently press Approve.

### 3.5 Use of card number, expiry date and security code

When you use the card for purchases, e.g. online, you must state the card number, the card's expiry date and the security code.

If the store is registered for 'Verified by Visa' or 'Dankort Secured by Nets' (cf. section 6), you must also enter the one-off code you will receive via text message in connection with the purchase. This code is the store's guarantee that the card holder is in possession of the card when payment is made.

When you use the card for mail order and phone order purchases, you must state the card number, the card's expiry date, the security code and your name and address, as required. For mail order purchases, you must also sign the order form.

Never provide your PIN code in connection with online purchases or in connection with mail orders or phone orders, etc.

### 3.6 Pre-registration of card details

You have the option of registering your card details with the individual store or with a digital wallet provider, so that you do not need to enter your card details when approving future online purchases. Follow the instructions from the store or the provider of the digital wallet.

On Dankort's website – <http://dankort.dk/Pages/Dankort-i-apps.aspx> – you can see which digital wallets and unique device IDs have been approved and for which you can register a Dankort.

You can make an agreement with a store that your card details will be registered for the purpose of paying for a subscription or other recurring purchases. The store will draw the agreed payments and you will thus not have to approve each payment. When you use your card details in this way, always ensure that you can cancel the subscription again, and make a note of the terms and conditions that apply.

If your card is replaced, you must update your card details yourself for venues where your card is registered and where you wish to continue to be able to pay without authorisation. This does not take place automatically.

## 4. Storage of Visa/Dankort and PIN code

### 4.1. Cards

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

Your card cannot be transferred or assigned to anyone else. This also applies to Dankort on mobile – but with limited withdrawal rights, as for cards in wallets.

### 4.2. PIN code

Your PIN code is personal and may only be used by you. You will receive a PIN code for your card automatically. When you receive the PIN code, you must certain that nobody else could have had access to the code.

Learn your PIN code by heart. Do not keep your code with your card, write it on the card, or save it on or with your mobile phone.

Do not disclose your PIN code to anyone else or otherwise allow anyone else to learn the code. When you enter your PIN code, always make sure that no one else can read your code.

If you suspect that someone else has had access to your PIN code, you must contact your bank immediately.

If you cannot learn the code by heart or want to store it, always do so responsibly. If you need to write your PIN code down, you should use a PIN code reminder device that you can obtain from your bank.

## 5. Power of attorney

If you want another person to be able to make withdrawals from your account using a Visa/Dankort, that person must hold power of attorney for your account and have their own card with their own PIN code. Their use of your card is in accordance with the same rules as apply to you. However, there are special rules for Dankort on mobile with limited withdrawal rights – cf. section 2.10.

Remember to inform your bank if you no longer want the other person to be able to withdraw from your account. The bank will cancel the power of attorney and confirm blocking/return of the card.

## 6. Secure Internet payments

'Verified by Visa' and 'Dankort Secured by Nets' are an extra safeguard against misuse of card details when shopping online. They also mean that when shopping online, you will need a one-off code that you will receive from Nets via text message in connection with payment in addition to your card. Another safeguard may be that when shopping online, you will have to use your NemID to approve payment after entering your card details. This applies if you have not registered your card for 'Verified by Visa' or 'Dankort Secured by Nets', or if you have a new mobile number – cf. section 6.1.

### 6.1 Registration

Before you make your first purchase from a store using 'Verified by Visa' or 'Dankort Secured by Nets', you must register your card.

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

Registration can be made either via your bank's website or online banking. Registration is made using your NemID.

When registering, you must also specify the mobile phone number on which you want to receive one-off codes. You can change the registered phone number either via your bank's website or online banking.

If you have not registered your card for 'Verified by Visa' or 'Dankort Secured by Nets', you can shop using NemID.

Please note that not all Dankort transactions will require 'Dankort Secured by Nets', even if the store displays this sign. Minor transactions can often be made without using 'Dankort Secured by Nets'.

### 6.2 Security – card and phone

As your mobile phone becomes part of the security measures for online purchases in stores that use 'Dankort Secured by Nets' or 'Verified by Visa', always ensure that no one else has or can gain unhindered access to your card and your mobile phone. We therefore recommend that you use a code for your mobile phone.

Always change/cancel your mobile phone number as soon as possible if you lose the phone on which you receive one-off codes. You must also block your card if you lose it, cf. section 10.

## 7. Checking account entries

You are obliged to check the entries on your account regularly. If your check reveals transactions that do not correspond to your receipts, or transactions you do not believe that you have made, contact your bank immediately. If necessary, you can use the secure communication channel provided by your bank, e.g. via online banking. When checking entries, remember that when you use your card for online purchases, mail orders or phone orders, the store cannot deduct the amount until the item has been sent in principle. When buying e.g. airline tickets or concert tickets, however, the store will deduct the amount at the time of booking.

In this connection, you should be aware of the deadlines in sections 8 and 9 concerning the reimbursement of payments.

## 8. Reimbursement of payments that you have approved

### 8.1 If you did not know the final amount at the time of approval

If you did not know the final amount when you approved the payment and the amount subsequently drawn from your account is significantly higher than could reasonably be expected, you may be entitled to reimbursement of the payment. This may e.g. be the case in connection with car hire or check-out from hotels, where you have approved that the store can subsequently charge for e.g. fuel or minibar.

You must contact your bank no later than eight weeks after the amount has been drawn from your account if you believe that you are entitled to reimbursement of a payment for which you have not approved the final amount.

### 8.2 Online purchases, mail orders and phone orders, etc..

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

- online purchases and purchases via mail order or phone order,
- purchases for which the card was not read, but where you have provided card details (card number, etc.) for the purpose of completing the transaction, or
- purchases from self-service vending machines without a PIN code,

you may be entitled to reimbursement, if:

- the store has deducted a higher amount than agreed
- the item/service ordered has not been delivered
- if, before the goods or services are delivered, you exercise an agreed or statutory right of cancellation.

You must first seek to resolve the problem with the store before contacting your bank. You must be able to prove that you have contacted or attempted to contact the store – e.g. via emails/letters.

It is a condition that you contact and complain to the bank as soon as possible after you have become (or should have become) aware that one or more amounts have been wrongly withdrawn from your account. As far as possible, you must complain no later than 14 days after you have become (or should have become) aware of your potential claim. When assessing whether you have complained in due time to the bank, whether you have fulfilled your obligation to check entries on your account regularly will be taken into account, cf. section 7.

After receiving your complaint, the bank will investigate the transaction and your complaint. While your complaint is being investigated, the amount in dispute will normally be credited to your account. If the complaint subsequently proves to be unjustified, the bank will withdraw the amount from your account again.

If your complaint proves to be unjustified, the bank may charge interest for the period in which the amount was deposited to your account and until the amount is withdrawn, as well as a fee for requesting proof of purchase in-store, e.g. a copy of the transaction receipt – cf. the price list.

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

## 9. Reimbursement of payments that you have not approved

If you believe that one or more payments have been made using your Visa/Dankort that you have not approved, contributed to or made, contact the bank as soon as possible after becoming aware of the unauthorised transaction. You must contact your bank no later than 13 months after the amount has been deducted from your account.

Your bank will then investigate your complaint. While your complaint is being investigated, the amount in dispute will normally be credited to your account. If the complaint subsequently proves to be unjustified, the bank will withdraw the amount from your account again. If the investigation shows that someone else made unauthorised use of the card, the bank may be able to hold you liable, cf. section 11.

If your complaint proves to be unjustified, the bank may charge interest for the period in which the amount was deposited to your account and until the amount is withdrawn, as well as a fee for requesting proof of purchase in-store, e.g. a copy of the

transaction receipt – cf. the price list.

## 10. Your duty to block the card

### 10.1 Cards

Contact your bank as soon as possible to block your card if:

- You lose your card
- Someone else becomes aware of your PIN code
- You discover that the card has been misused
- You suspect that the card has been copied
- You otherwise suspect that the card could be misused.

If you need to block your card outside the bank's business hours, contact Nets on (+45) 44 89 29 29, which is a 24-hour service. When you contact Nets, state your name and address, the bank/branch at which the account is held and, if possible, the card number, account number or CPR number.

When the card has been blocked, you will be informed, stating the reason and time. Please note that when your card is blocked, you cannot use your card in wallets.

If a blocked card is found again, contact your bank and agree with them how you should proceed. In certain circumstances, your bank may be able to cancel the blocking.

### 10.2 Card in wallet (e.g. Dankort on mobile)

A card on your mobile must be blocked in the same way as your physical card if

- You lose your mobile phone
- You discover that your card on mobile has been misused
- You otherwise suspect that your card in a wallet (e.g. Dankort on mobile) could be misused.

If you need to block your card on mobile outside the bank's business hours, contact Nets on (+45) 44 89 29 29, which is a 24-hour service. When you contact Nets, state your name and address, the bank/branch at which the account is held and, if possible, the card number, account number or CPR number.

When your card in a wallet has been blocked (e.g. Dankort on mobile), you will be notified of the reason and time.

If a mobile phone with a blocked card on mobile is found again, contact your bank and agree with them on how to proceed. If someone else becomes aware of the PIN code of the wallet(s) in which you have registered your card, change the PIN code as soon as possible. Follow the instructions in your wallet and contact the bank for further information on how to proceed.

## 11. Your liability in the event of misuse of your Visa/Dankort

### 11.1 Covering losses

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

### 11.2. Liability and own risk

If your Visa/Dankort has been misused by another person and a PIN code has been used, you must cover up to DKK 375 of the total loss.

You must pay a maximum of DKK 375 in total if several of your cards with the same PIN code are misused in connection with the same incident. However, this requires that all cards are blocked at the same time.

You must cover losses up to DKK 8,000 if your Visa/Dankort has been misused by another person and your PIN code has been used, and

- you have failed to inform the bank as soon as possible after becoming aware that the card or your mobile phone with the wallet containing e.g. Dankort on mobile has been lost, or that unauthorised persons have become aware of the code,
- you have intentionally disclosed your PIN code to the person who made the unauthorised use, but you did not realise, or ought to have realised that there was a risk of misuse, or
- you have enabled unjustified use through grossly irresponsible behaviour.

However, you will not have to pay more than DKK 8,000 in total if several of your cards with the same PIN code are misused in connection with the same incident. This requires that all cards with the same PIN code are blocked at the same time.

### 11.3. Liability for full loss

You are liable for the full loss if your PIN code has been used in connection with misuse under the following conditions:

- You have personally disclosed your PIN code to the person who has misused your Visa/Dankort AND
- You realised or should have realised that there was a risk of misuse.

You will furthermore be liable for the full loss if you have acted fraudulently or deliberately failed to fulfil your obligations in accordance with these rules, including keeping your card or mobile phone secure, protecting the PIN code, cf. section 4, or blocking the card, cf. section 10.

If you have several cards with the same PIN code, unlimited liability applies in accordance with section 11.3 and for each card that is misused.

## 11.4. Non-liability

You are not liable for losses arising after the bank has been informed that the card must be blocked.

Nor are you liable for losses if you were unable to block your card due to circumstances at the bank. You are not liable if the loss, theft or unauthorised appropriation of the 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 due to actions by the bank's employees, agents or branches, or by an entity to which the bank's activities are outsourced, or their failure to take action.

The bank is liable for your loss in accordance with the Danish Payment Services Act if the payee knew or should have known that unauthorised use had been made of the card.

The bank is also liable under the Danish Payment Services Act if you suffer losses as a consequence of unauthorised use for which the bank does not require the use of a PIN code, unless you have acted fraudulently.

You are only liable for losses as a consequence of unauthorised use of the card by someone else if the transaction has been registered and booked correctly by the bank.

## 12. Rights and responsibilities of the bank

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

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

- if the account to which your card is linked has been closed
- if you breach the rules, including if the account to which the card is linked is overdrawn
- if your Visa/Dankort has been misused or is suspected to have been misused by a third party.

In the event of an overdraft, you will receive a written reminder before the card is blocked. However, immediate blocking without prior contact may be necessary in the case of particularly high and/or repeated excess spending.

The bank may also require the return of all cards issued for the account.

When the bank has blocked your Visa/Dankort, you will be informed, stating the reason for and time it was blocked.

In the event of suspected or actual cases of misuse or security threats, the bank may contact you by phone or by other secure means.

### 12.2 Replacement of the card

The bank has the right to replace the card at any time.

### 12.3 The bank's liability

The bank will be liable if it fulfils its contractual obligations too late or incompletely, as a consequence of errors or omissions.

The bank is not liable for losses as a consequence of:

- disruption of/lack of access to IT systems or damage to data in these systems that can be attributed to the events described below, irrespective of whether the bank itself or an external supplier is responsible for operation of those systems
- failure of the bank's power supply or telecommunications, legislative measures or administrative acts, natural disasters, war, riots, civil unrest, sabotage, terrorism or vandalism (including computer virus and hacking)
- strike, lockout, boycott or blockade, irrespective of whether the dispute is directed at or initiated by the bank itself or its organisation, and irrespective of the cause of the dispute. This also applies when the dispute solely affects parts of the bank
- other circumstances beyond the control of the bank.

The bank's exemption from liability will not apply if:

- the bank should have foreseen the circumstances that caused the loss when the agreement was entered into, or should have avoided or overcome the cause of the loss
- legislation renders the bank liable for any circumstances causing the loss.

## 12.4 Industrial disputes

You cannot use your Visa/Dankort in Denmark if the bank and/or its data centre is involved in an industrial dispute. On commencement and termination of any such dispute, you will be notified as soon as possible, including by advertising in the national press and/or information via the bank's website.

You cannot expect to be able to use the card outside Denmark if the bank's data centres and/or one or more of its international partners are involved in an industrial dispute. In the event of industrial disputes solely outside Denmark, your Visa/Dankort may continue to be used in Denmark.

## 12.5 Errors and omissions

The bank is not liable for errors and omissions, etc. in the services provided by a store. Any complaints concerning errors and omissions in the services delivered must be addressed to the store.

## 13. Expiry

You may use the card up to and including the expiry date shown on the card, after which the card will be invalid. Dankort on mobile will expire at the same time as the card to which it is linked. Before the card expires, you will receive a new card or details on how you can collect a card.

## 14. Termination

The bank may terminate the agreement with two months' notice. In the event of termination, you will be refunded a proportional share of any fees you may have paid prior to using the card.

You can terminate the agreement with your bank with one month's notice.

If you terminate the agreement before the end of the first six-month period, the bank may charge a fee for termination of the agreement, cf. the price list.

If you or the bank terminate the agreement, the card must be returned. If you send the card by post, it must be cut up before sending.

## 15. Changes to the rules

Changes to the rules and price list can be made with two months' notice, if the changes are to your disadvantage.

Changes to your advantage may be made without notice. You will receive notification of changes either in writing or electronically. You are obliged to notify any changes in your address and/or email address to the bank, and you are responsible for your non-receipt of notification of changes, if you have not notified us of any change of email or postal address.

Any change in the rules will be deemed to be adopted unless you inform the bank before the date of entry into force that you do not wish to be bound by the new rules.

If you notify that you do not wish to be bound by the new rules, the agreement will be deemed to have expired on the date of entry into force of the new rules. If you have prepaid the fee for one year, a proportional share will be reimbursed to you.

## 16. Complaints

If you have any complaints, please contact your bank. If your complaint is not successful, you can contact the Danish Complaint Board of Banking Services (Amaliegade 8B 2nd floor, DK-1256 Copenhagen K – [www.fanka.dk](http://www.fanka.dk)) or the Consumer Ombudsman (Carl Jacobsensvej 35, DK-2500 Valby – [www.forbrugerombudsmanden.dk](http://www.forbrugerombudsmanden.dk)).

You can also complain to the authorities that supervise the bank's compliance with the Danish Payment Services Act. The Consumer Ombudsman supervises disclosure requirements concerning the performance of payment services, rights and

obligations on using payment services, the use of payment data and information concerning fees. The Danish Competition and Consumer Authority (Carl Jacobsensvej 35, DK-2500 Valby – [www.kfst.dk](http://www.kfst.dk)) oversees the rules for fees in general

If you wish to complain that your card has been blocked, you can also contact the bank. If your bank does not uphold your complaint, you can appeal to the Danish Data Protection Agency (Borgergade 28 5., DK-1300 Copenhagen K – [www.datatilsynet.dk](http://www.datatilsynet.dk)).



## 17. New copy of the Visa/Dankort Rules

If you lose your copy of the Visa/Dankort Rules, or require a new copy for any other reason, you can find the Rules on your bank's website, or contact the bank directly.

## 18. Fees and currency conversion

### 18.1 The bank's fees

Any fees are stated on the bank's website and in the price list. This will also state when collection will take place and whether the fee will be collected in advance.

### 18.2 The store's fees

When using your Visa/Dankort abroad and on foreign online sites, the store may charge a fee.

### 18.3 Exchange rate when using the card abroad

Purchases and withdrawals abroad are converted to Danish kroner, cf. the price list. The amount will always be drawn from your account in Danish kroner.

The methods described in the price list are used for the conversion, see the 'conversion rate' section of the price list. Changes to the conversion rate stated in the price list will enter into force without notice.

There may have been changes in the exchange rate during the time from when you used your Visa/Dankort until the amount is deducted from your account. Some countries, primarily outside Europe, may have several official exchange rates, depending on from where the exchange rate is obtained.

### 18.4 Currency conversion in a store abroad (Dynamic Currency Conversion)

If you use the card abroad, the store may offer currency conversion before payment takes place, so that you pay an amount in Danish kroner. Before you approve the amount, the store must state which fees and exchange rate the store will use for the conversion. Please note that the exchange rate used by the store may differ from the exchange rate used by your bank.

The bank has no influence on the conversion rate used by the store.

## 19. Assessment of card applicant

Visa/Dankort is issued on an individual basis.

## 20. Consent to the use, storage and disclosure of information

By accepting these rules and using Visa/Dankort, you consent to the processing of personal data. When a card is used, information such as the card number, amount, date of use and where your card was used is considered to be personal data.

Data concerning you is solely processed for purposes that are necessary for you to be able to use the card as agreed, including the transaction of payments. The data is processed in accordance with the data protection regulation, including the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council).

The data is retained by the store, the store's bank and their data provider (e.g. Nets) and is retained by your bank for bookkeeping purposes, account statements and any subsequent correction of errors. When you use the Visa part of your Visa/Dankort, the data for the purpose of completing your payment will also be stored by Visa Inc., which is obliged to store and process the data in accordance with the EU General Data Protection Regulation.

Data is only disclosed when required by legislation or to prevent misuse of the card. The data is stored for the current year plus five years.

When registering for 'Dankort Secured by Nets' and 'Verified by Visa', your mobile number is retained by Nets for the purpose of sending out one-off codes.

You can withdraw your consent to the processing of your personal data at any time by contacting your bank. If you withdraw your consent, however, you should note that you will no longer be able to use the card.

If you are dissatisfied with the processing of your personal data, you can complain to the bank or the Danish Data Protection Agency, Borgergade 28, 5., DK-1300 Copenhagen K (email: dt@datatilsynet.dk)

If you have any questions about the processing of your personal data, you are always welcome to contact the bank's data protection officer. Here, you can also get information about Visa Inc.'s processing of your personal data.

## 21. Registration of blocked Visa/Dankort

If your Visa/Dankort has been blocked, cf. sections 10 and 12, this will be registered in the banks' joint register of blocked Dankort and Visa/Dankort cards. Blocked Visa/Dankort cards will also be included in Visa's list of blocked cards.

The joint Dankort register is available to banks and stores that receive Visa/Dankort payments, so that they can check whether a card used for payment has been blocked.

## 22. Supervision

The bank is subject to the supervision of the Danish Financial Supervisory Authority and is registered in the bank register under registration number 0880.

## 23. Glossary

### Banking Day:

All days except Saturdays, Sundays and public holidays, Friday after Ascension Day, Danish Constitution Day, Christmas Eve and 31 December.

### Dankort on mobile:

A virtual version of the Dankort part of your Visa/Dankort, which can be linked to a wallet on your mobile phone.

### Dankort on mobile with limited withdrawal rights:

Dankort on mobile with limited withdrawal rights is a solution whereby the card holder links a limited withdrawal right to a virtualised card, and gives another person (typically a child) access to use the limited, virtual card. The card holder sets the limits for use of the virtual card. There will always be maximum limit for use, set by Dankort (Nets). The virtual card with limited withdrawal rights functions in the same way as an ordinary Dankort on mobile at the time of payment.

### Dankort Secured by Nets:

Dankort Secured by Nets is an extra safeguard from misuse of card details when shopping online.

### Digital wallet:

A digital wallet is a personal software-based solution whereby you register your card details for future online purchases in an online store.

### Dynamic currency conversion:

Used by some stores, so that you can pay abroad in Danish kroner. The currency conversion is performed by the store, and the card holder's bank has no influence on the exchange rate used for the conversion.

### Loyalty programmes:

Loyalty programme is a collective term for solutions whereby the card holder can link his/her card to a provider of an loyalty programme and then use the card to either earn bonus, etc. or be part of a donation scheme.

### Store:

All stores, hotels, restaurants or other venues that accept payment with Dankort and/or Visa.

### One-off code:

A code that you receive via text message to the registered mobile phone. You must use the code that is sent for purchases in stores that use Dankort Secured by Nets or Verified by Visa.

### Contactless payment:

Contactless payment is payment using the card's chip without having to insert the card in the card terminal. When you pay, you simply hold the card at a distance of 0-3 cm from the card terminal's contactless symbol.

### Card:

The physical card.

### Receipt:

Payment details on paper or in electronic form.

### NemID:

NemID is a digital signature. A technical distinction is made between NemID that you use in your bank, and NemID with an OCES certificate, 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 code:

The personal secret code that is linked to your physical card and the personal secret code you have chosen for your Dankort on mobile.

**Price list:**

The current list of fees, etc. You can obtain the price list from your bank.

**Conversion rate:**

The exchange rate used for the conversion of payments in foreign currency to Danish kroner.

**SSL:**

SSL is the abbreviation for Secure Sockets Layer. SSL is an encryption standard used to protect data during online transmission.

**Transaction:**

Designation of cash withdrawals or individual purchases in shops, online stores, or similar.

**Unique device ID:**

Unique device ID is used in payment software that has security approval in accordance with the PCI standard and where the card holder can save parts of their card details.

When the card holder needs to make a payment to an online store, the card holder can retrieve the saved card details, and then only needs to enter security code (CVC/CVV), which are the code from the back of the payment card, in order to approve the payment.

**Verified By Visa:**

Verified by Visa is an extra safeguard against misuse of card details when shopping online.

**Visa:**

The organisation that determines the international rules for the Visa system.

**Visa/Dankort:**

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

**Wallet provider:**

Provider of a wallet in which a Dankort can be registered for mobile use.

**Wallet:**

A personal, software-based solution which can contain your Dankort on mobile or other virtual cards, for example. A wallet is like an app that you can download to your mobile phone.

## **Good VISA/Dankort advice**

Payment cards are one of the most secure means of payment available. By following this advice, you can help to ensure even greater security.

### **1. General advice on your Visa/Dankort**

#### **Before use**

- Regard your Visa/Dankort as cash. You should therefore keep it safe both at home and when you are out and about. Do not leave it lying around.
- Learn your PIN code by heart. Use a PIN code reminder if you are not sure whether you will always be able to remember the code. You can contact your bank to request a PIN code reminder device.
- Never give your PIN to anyone else – not even the bank or the police. The code is personal and only you must know it.
- Do not use your PIN code as a password or access code in any other context.
- Protect your devices on which you have installed your digital wallet. Make sure the device is always updated with the latest version and that a code is needed to open your mobile phone.
- It is important that you have an antivirus program and an operating system that are kept updated, and that you use your common sense when surfing online, checking emails, and so on.

#### **During use**

- Protect your PIN code when you enter it. Do not allow anyone else to read the code when you enter it.
- Decline assistance from 'friendly helpers' when using your card.
- Never allow anyone else to use your card or PIN code – even if you are present.
- Check that the total amount shown on the terminal is correct.
- Never sign a receipt before the total amount has been added.
- Remember your receipt and save it for checking later.
- Protect the card's magnetic stripe. The information in the card's magnetic stripe can be damaged if it comes too close to a magnetic field, e.g. a magnetic lock on a bag and certain electronic devices.

#### **After use**

- Check the entries on your account – via your online bank or the account statement.
- Check regularly that you have not lost the card.

React immediately if your card is lost or you suspect it may have been misused. Contact your bank as soon as possible [*or Nets*].

### **2. Using Visa/Dankort abroad Use**

#### **your PIN code with care**

When you are abroad, you may only use your PIN code in ATMs, vending machines and stores that display a Visa logo sign.

#### **Remember your passport or other photo ID**

Foreign banks will often ask for a passport if you want to withdraw cash at the cashier's desk. You may also be required to present proof of identity in stores.

### **3. Good advice when shopping online**

Payment cards are also safe to use when shopping online. You can help to maintain your own security by following these guidelines.

Below is some general advice concerning shopping online.

#### **3.1. General advice concerning shopping online**

##### **Read the terms and conditions**

If you wish to make a purchase, read the terms of sale carefully. Make sure that with this single purchase you do not unintentionally open an account or agree to additional payments.

##### **Save the documentation**

When you have ordered an item, save any documentation from the purchase either as a print or by making an electronic copy of the screen. Also remember to save both the store's web address and the address of the page where the purchase/subscription can be cancelled, if necessary.

The online store is obliged to acknowledge the purchase, e.g. via an email. Remember to also save this receipt.

##### **Check entries on your account**

If you have an online banking agreement, you can monitor the entries on your account regularly. If this is not the case, check your account statements. If there are entries that you do not recognise, contact your bank immediately.

## 3.2. Special advice for shopping online using

### Visa/Dankort Protect your card number

Never disclose your card number unless you are in a specific purchase situation where you want to pay for something. In other situations, you must never enter your card number, even if you are asked to do so, either as ID, as part of 'member details' or to progress to another page.

### Data protection

All Danish online stores must use encryption to protect your payment details. Most foreign stores also use encryption, and it is easy to check whether the connection between your computer and the online store is secure. If the connection is secure, there will be a padlock in the bottom right-hand corner of your web browser or preceding the URL (web address) shown in green. Do not enter your card number, etc. until the connection is secure. Do not shop in stores that do not offer an encrypted connection.

### Online store accounts

When joining an account scheme, you permit the online store to charge your card without any action by you. Always carefully check the terms and conditions of payment using such an account in detail before stating your card number, etc.

### New Visa/Dankort

When your Visa/Dankort has to be renewed, the card number will be changed. If you have accounts with stores such as Brobizz, MobilePay, Netflix, Rejsekort or mobile subscription, you will need to inform the store in question of the new card number, in order for the account to continue.

## 3.3. Where can I read more?

You can read more about online shopping on the following websites:

- [www.forbrugersikkerhed.dk](http://www.forbrugersikkerhed.dk)
- [www.forbrug.dk](http://www.forbrug.dk)

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

Always report a lost or stolen Visa/Dankort immediately. If you suspect that your PIN code has been read or that someone else is using your card or card number unlawfully, this must always be reported. Contact your bank immediately, so that your Visa/Dankort is blocked and cannot be used.

Outside the bank's business hours you must contact Nets on (+45) 44 89 29 29, which is a 24-hour service. When you contact Nets, state your name and address, the bank/branch at which the account is held and, if possible, the card number, account number or CPR number.

## 5. Contacting your bank

When you need to contact your bank, always use the secure communication method recommended by the bank – e.g. via your online bank or by telephone. Communicating with your bank in this way ensures that no one can read your correspondence.

*Excerpt from the Danish  
Payment Services Act no.  
652 – 8 June 2017 Rules  
concerning liability*

**Section 99.** The payer's provider of payment services will be liable in relation to the payer for losses as a consequence of unauthorised payment transactions, cf. Section 97, unless otherwise stated in Section 100. In the event of an unauthorised transaction, the payer's provider shall repay the amount immediately and no later than the end of the following working day, unless the payer's provider has reasonable grounds to suspect fraud and informs the Danish Financial Supervisory Authority of these reasons.

(2) When an unauthorised payment transaction is initiated via a payment initiation service provider, the account-holding provider shall reimburse the payer immediately and by no later than the end of the following working day, in accordance with subsection 1.

(3) When the provider of payment initiation services is liable for the unauthorised payment transaction, the payment initiation service provider shall, at the request of the account-holding provider, immediately indemnify the account-holding provider for any loss or amount paid as a consequence of the repayment to the payer, cf. Section 98(3).

(4) The Danish Financial Supervisory Authority lays down more detailed rules on the technical execution of the notification, cf. subsection 1, second sentence.

**Section 100.** The payer's provider of payment services shall be liable to the payer for losses incurred as a consequence of the unauthorised use of a payment service by someone else, unless otherwise provided in subsections 2-5. The payer will only be liable in accordance with subsections 3-5 if the transaction has been correctly registered and booked, cf. subsection 2, however.

(2) The payer is liable, without limitation, for losses incurred as a consequence of the payer acting fraudulently or intentionally failing to fulfil its obligations in accordance with Section 93.

(3) Unless further liability arises from subsections 4 and 5, the payer will be liable for an amount of up to DKK 375 for losses resulting from unauthorised use of the payment service by someone else, if the personal security measure connected to the payment service has been applied.

(4) Unless further liability arises from subsection (5), the payer will be liable for an amount of up to DKK 8,000 for losses resulting from unauthorised use of the payment service by someone else, if the payer's provider proves that the personal security measure connected to the payment service has been applied, and

1) that the payer has failed to inform the payer's provider as soon as possible after becoming aware that the payment instrument connected to the payment service has been lost or that the personal security measure has come to the knowledge of the unauthorised party,

2) the payer has deliberately surrendered the personal security measure to the person who carried out the unauthorised use, without the matter being subject to subsection 5, or

3) the payer's grossly irresponsible conduct made the unauthorised use possible.

(5) The payer will be liable, without limitation, for losses incurred as a result of unauthorised use of the payment service by someone else when the personal security measure connected to the payment service has been applied and the payer's provider proves that the payer has intentionally disclosed the personal security measure to the person making the unauthorised use and that this has taken place in circumstances where the payer realised or should have realised that there was a risk of misuse.

(6) Notwithstanding subsections 3-5, the payer's provider will be liable for any unauthorised use which takes place

1) after the provider has been informed that the payment instrument connected to the payment service has been lost, that an unauthorised person has become aware of the personal security measure, or that the payer wishes the payment instrument to be blocked for other reasons,

2) where it is caused by the actions of a provider's staff member, agent or branch, or by an entity to which the provider's activities have been outsourced, or their lack of action, or

3) because the provider has not taken appropriate measures, cf. Section 94(1), 2).

(7) Notwithstanding subsections 3-5, if the provider does not require strong customer authentication, the payer's provider will also be liable, unless the payer has acted fraudulently. The payee or their provider will reimburse the losses incurred by the payer's provider if the payee or their provider has failed to use strong customer authentication. The first and second sentences do not apply to services that are subject to Section 1(5) and Section 5, 14)-16).

(8) Notwithstanding subsections 3-5, the payer's provider will also be liable if the loss, theft or unauthorised appropriation of the payment instrument connected to the payment service, or the personal security measure connected to the payment service, could not have been discovered by the payer prior to the unauthorised use.

(9) Irrespective of subsections 3-5, the payer's provider will also be liable if the payee knew or should have known that the use of the payment service was unlawful.

(10) Subsections 1-9 will also apply to electronic money, unless it is not possible for the payer's issuer of electronic money to block the payment account or payment instrument

**Section 101.** A payer will be entitled in relation to the provider to reimbursement of the full amount for an executed payment transaction that has been initiated by or via the payee, provided that:

1) the payer has not approved the exact amount of the payment transaction and

- 2) the payment transaction exceeded the amount which the payer could reasonably expect, taking into account, inter alia, the payer's previous expenditure pattern and the terms of the framework agreement.
- (2) Changes in the exchange rate, when calculated on the basis of a reference rate, may not be invoked on the application of subsection 1, 2).
- (3) It may be agreed in the framework agreement between the payer and the payer's provider that the payer is not entitled to reimbursement under subsection 1 if consent to execute payment transactions subject to subsection 1 has been given directly to the payer's provider and information concerning the future payment transaction was given or made available by the provider or the payee to the payer at least four weeks before the due date.
- (4) In the case of direct debits, the framework agreement between the payer and the payer's provider may state that the payer is entitled to reimbursement from their provider, even if the requirements under subsection 1 are not fulfilled.
- (5) Notwithstanding subsections 1 and 2, the payer will be entitled to unconditional reimbursement for direct debits subject to Article 1 of Regulation (EU) no. 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro.

**Section 102.** A request for reimbursement, cf. Section 101, must be received by the provider no later than eight weeks after the payment transaction in question is debited.

- (2) The payer's provider shall, within ten working days of receipt of a request for reimbursement, either reimburse the entire amount of the transaction or justify a refusal of repayment, with information on access to complain. (3) Notwithstanding subsection 2, the provider may not refuse to reimburse direct debits, cf. Section 101(5).

*The entire text of the Act can be found at [www.retsinformation.dk](http://www.retsinformation.dk)*

*Updated October 2020*