Card conditions for Visa/Dankort

Applicable from 1 April 2024

The conditions that apply to Visa/Dankort cards are set out below.

The conditions that apply to Visa/Dankort cards are set out below.

1 Visa/Dankort card conditions

These conditions apply to the use of Visa/Dankort cards in and outside Denmark. The conditions apply irrespective of whether the card is used for purchases in a physical shop or for online purchases.

The conditions apply to Visa/Dankort cards, both physical cards and virtual cards in a digital wallet. Definitions of terms used are listed at the end of this document.

2 Use of the Visa/Dankort card

The Visa/Dankort card is a payment instrument for use with merchants that accept the card in and outside Denmark.

If a merchant accepts both Visa and Dankort cards, the merchant may have chosen either Dankort or Visa as the merchant's preferred method of payment. In accordance with applicable legislation, the merchant must ensure that you can change the merchant's choice and pay with the part of the card that you want. You change the choice via the payment terminal. The entries in your account will specify whether a payment has been completed as a Dankort or a Visa transaction.

Please note that international Visa card payments may be subject to fees and charges, and that the monthly spending limit on your Visa card is reduced by the transaction amount. This applies also if you use the Visa part of your Visa/Dankort card in Denmark (see 2.8).

2.1 Cash withdrawals

You may use either your Dankort card or your Visa card to withdraw cash from ATMs that accept Dankort and/or Visa cards. You may also use the Dankort part of your card for cash withdrawals at the cashier's desk at selected Danske Bank branches and at the branches of most other banks in Denmark as well as the Visa part of your card at banks that accept Visa.

Please note that not all ATMs in Denmark accept the Dankort card. In such case, the withdrawal will be made using the Visa part of your card and may thus be subject to a fee.

Visa card fees and any amount limits are stated in the tariff of charges.

Danske Bank A/S
CVR-nr. 61 12 62 28 - København

2.2 Purchases from merchants

You may use your Visa/Dankort card to pay for goods and services provided by merchants accepting the Dankort card and/or the Visa card.

You may also use your card to make online purchases as well as purchases by mail order and telephone order. Furthermore, you can use your Visa/Dankort card to make payments at self-service machines.

Dankort and/or Visa logos at merchants or on websites tell you whether merchants accept the Dankort card and/or the Visa card.
A merchant can make a refund into your card account through your Visa/Dankort card.

You may not use your Visa/Dankort card for illegal purposes, including purchases of goods or services considered illegal under local legislation.

In connection with Visa card payments abroad, you may be asked to choose whether the payment should be made in local currency or in Danish kroner (see 18.4 for further details).

2.3 Approval of account transfers via Danske Bank's ATMs

You may use your card to approve account transfers made via Danske Bank's ATMs to accounts with Danske Bank and to accounts with other banks in Denmark.

2.4 Debits to your account

As a general rule, purchases and cash withdrawals (transactions) made using your Dankort card are debited to your account on the day you use the card. If you have made a payment using the Visa part of your card, the transaction will be listed on the card account the day after the purchase or cash withdrawal at the earliest. The time at which the amount is debited to your account will, however, depend on when we receive the transaction.
Unless otherwise agreed, purchases and cash withdrawals may not exceed the balance in your account (see clauses 2.6-2.10).

2.5 Contactless payment or card in a digital wallet

When you use contactless payment or a digital wallet, an amount limit determines whether or not you need to enter your PIN. For information on the amount limit, please visit www.danskebank.dk. The amount limit may change. You will not receive notification if the limit is raised or lowered less than 50% within a calendar year.

If the payment exceeds the applicable amount limit, you will automatically be asked to authorise the payment by entering your PIN on the payment terminal or by authorising the payment on your mobile phone. You are asked to enter your PIN at regular intervals, even if the amount does not exceed the applicable amount limit.

2.6 Gambling and lottery

When you use your Visa/Dankort card at shops that provide gambling and betting services – that is, when you use your card at casinos, for buying lottery tickets, on race courses and the like – a daily spending limit may apply. The tariff of charges, which is available at www.danskebank.dk/priser, specifies this limit.

2.7 Cash withdrawals

Visa/Dankort cards are subject to a daily cash withdrawal limit. The amount is stated in the tariff of charges.

2.8 Visa – spending limits

Your Visa card is subject to an overall limit on purchases and cash withdrawals over a 30-day period. Within this overall limit, maximum amounts apply to per day cash withdrawals from banks and ATMs. The tariff of charges, which is available at www.danskebank.dk/priser, specifies these amounts.

2.9 Miscellaneous

The individual merchant may set limits for use of the card.

Some banks and ATMs may set limits specifying the maximum amount of cash you may withdraw. You may have to pay a fee every time you withdraw cash, regardless of the amount withdrawn.

Danske Bank A/S
CVR-nr. 61 12 62 28 - København

2.11 Loyalty programmes
You can register the Dankort card and the Visa card for various loyalty programmes. The Dankort card may be registered only with loyalty programmes approved by Nets.
Go to this website to see the approved loyalty programmes:
http://dankort.dk/Pages/Loyalitetskort.aspx

3 Visa/Dankort card use

3.1 Payment
Before you authorise a payment or cash withdrawal, you must always check that the amount is correct. Payments that you have authorised cannot be revoked. See, however, clauses 8 and 9 regarding the possibility of reversing a payment.

You should always make sure to get a receipt for your transaction (in certain self-service machines, however, you do not get a receipt). You must make sure that the amount matches the amount of the purchase or cash withdrawal and that the date is correct. You should keep your receipt until you have verified that the amount debited to your account is correct (see clause 7).

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

Reading/checking of data on the card via
- the chip/magnetic strip and PIN
- the chip/magnetic strip and signature
- the contactless payment function
- the wallet
- the chip/magnetic strip but not the PIN at self-service machines

By entering information from the card (for example in connection with online purchases where data cannot be read digitally)
- By registering the card number, expiry date and card validation code (typically, where you enter the information yourself)

By registering card data in advance, for instance for
- agreements with individual merchants to register card data for use in connection with future payments authorised and initiated by you
- subscriptions under which the merchant charges amounts according to specific agreement with you
- agreements with providers of a digital wallet in which you register your card data for use in connection with future payments authorised and initiated by you

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

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

If you notice that a merchant issues more than one receipt stating your card details, you must make sure that any unsigned receipts are destroyed.

If you authorise a merchant to debit an additional amount (a service tip, for example) to your Visa/Dankort card, you must ask for a receipt for the full amount.

When you use your Visa/Dankort card to hire a car or pay for hotel accommodation, for example, you will often be asked to sign a receipt that allows the car hire company or the hotel to subsequently debit additional amounts. You must keep in mind that signing a receipt may allow the car hire company or the hotel to debit additional amounts to your account (see clause 8).

Merchants such as car hire companies and hotels can also reserve an amount through your card to cover the final invoice in full or in part. A merchant may reserve only the amount for which you have given your consent.

3.2 Contactless payment
If your card allows contactless payment, you can use the contactless payment function to make purchases at merchants offering that service. Contactless payment terminals allow you to use the card without inserting it into the payment terminal. Instead, you make the payment by holding the card close to the terminal (at a distance of 0-3 cm). Terminals with a contactless

function bear the following symbol:

An amount limit applies to each transaction made without entering your PIN (see clause 2.5).

At regular intervals, you will be asked to authorise the payment by entering your PIN even if the amount does not exceed the applicable limit for purchases made using the contactless payment function.

3.3 Cards in wallets

You may connect your Visa/Dankort card to a wallet app on your mobile phone and use this function to pay with the card.

You can register your Visa/Dankort card in all approved wallets that are open for Danske Bank-issued Visa/Dankort cards. Registration takes place by using your MitID (or similar security credentials). In the app, you can register the physical card you wish to use for payments. Furthermore, you will be asked to choose personalised security credentials, for example a PIN, to be used if a payment requires you to use personalised security credentials.

Information and guidelines on setup and use appear from the chosen digital wallet.

3.4 Self-service machines without PIN

At certain self-service machines, you can use your Visa/Dankort card without entering your PIN or signing a receipt. In such machines, you accept the transaction when your Visa/Dankort card is read by the machine or when you subsequently press the button to authorise the transaction.

3.5 Use of card number, expiry date and card validation code

You must enter the card number, expiry date and card validation code to make payments for online purchases, for example.

If the merchant uses Visa Secure or Dankort Secured by Nets, the special rules in clause 6 apply.
To make purchases by mail or telephone order, you must state the card number, expiry date, card validation code and, if required, your name and address. When you make a purchase by mail order, you must also sign the order form.

Never disclose your PIN or similar personalised security credentials in any of the above transactions.

3.6 Advance registration of card data

You can register your card data with a specific merchant or with a provider of a digital wallet so you will not have to enter your card data when authorising future online payments. You must follow the instructions provided by the merchant or the wallet provider.

Automatic card updating is a free service whereby your payment card details are automatically updated across a number of apps, webshops and subscriptions when you get a new card. This means that businesses with which you have registered your card details can obtain the new card details if they are not able to process the payment using the old card. If you no longer want your card details to be registered with a shop, you must remove the card details from your account with the shop in question.

If you do not want a regular payment to continue, you have to terminate the agreement with the relevant business.

The individual business decides whether it wants to register for automatic card updating with their payment solution provider. You may therefore still have to update your card details yourself with certain businesses. You will normally receive notification from the apps, etc. in which your card details are not updated.

4 Protection of your Visa/Dankort card and PIN

4.1 Card

Your card is personal and may be used only by you. When you receive your card, you must immediately sign it in the signature field on the back. You may not hand over or give the card to other persons.

This also applies if you have registered your card in a wallet.

4.2. Personalised security credentials

Your personalised security credentials, for example your PIN, are personal and may be used only by you. We send your card by physical post to the address that we have registered as your home address. To start using the card, you must activate it first. Just follow the instructions given in the letter.

The card will automatically be activated the first time you use it with the chip and the PIN at a merchant or an ATM.

You find your PIN in Danske Mobile Banking. If you have not logged on to Danske Mobile Banking for the past three months, we will send you a letter with a PIN unless you have decided to use the PIN of one of your other personal cards issued by Danske Bank.

Your PIN is generated and printed digitally without anybody seeing the combination. You must contact us immediately if the letter containing the PIN has been opened or is not intact.

You must always keep your card secure and check regularly that you have not lost it. Do not keep your PIN with your card or write it on the card. You should memorise your PIN and destroy the letter containing the PIN. Alternatively, you must keep the PIN in a secure place.

5 Authorisation to use your account

If you want another person to be able to withdraw amounts from your account using a Visa/Dankort card, that person must be authorised to operate your account and must have their own card with their own personalised security credentials/PIN.

The cardholder is subject to the same conditions as those applying to you.

If you want to revoke the cardholder's access to your account, the cardholder must return the card to us, and you must revoke the authorisation in writing.

6 Secure online payments

Visa Secure and Dankort Secured by Nets offer extra protection against unauthorised use of card data in connection with online purchases.
Visa Secure and Dankort Secured by Nets are normally used when you shop online, and it is the merchant that must offer this security solution. In some cases, the merchant may have chosen not to use Visa Secure and Dankort Secured by Nets.

In certain circumstances, Danske Bank is required to reject your payment if Visa Secure or Dankort Secured by Nets has not been used.

When you shop online with merchants using Visa Secure and Dankort Secured by Nets, you will be asked to enter a one-time password that you will receive from Nets by text message when you have entered your card details, and a password created by you.

Alternatively, you can use your MitID with the MitID code app to authorise the payment. This applies, for example, if your mobile number is not registered with us or your mobile number has changed (see 6.1).

Please note that not all card purchase transactions will require Dankort Secured by Nets or Visa Secure even though the merchant indicates that it uses such feature. Certain transactions in relation, for example, to transport and parking, can sometimes be completed without the use of security credentials.

6.1 How to register

When you receive your new card, it is automatically registered with Visa Secure and Dankort Secured by Nets.

Danske Bank uses the mobile number that you provided to us to send you the one-time password. If you change your mobile number, please update your contact information in Danske Mobile Banking or Danske eBanking.

If you have not registered your mobile number with us,

you can register it with Nets using your MitID.

You must create your password on Nets' website, www.nets.eu/3ds. You log on using your MitID or by requesting a one-time password, which is sent to you by mail.

6.2 Security – card, code and telephone
Since your mobile phone is an element of the added protection offered by Dankort Secured by Nets or Visa Secure when you shop online, you must make sure that others do not have and cannot get access to both your card and your mobile phone. We therefore recommend that you use a code to access your mobile phone.

If you lose the mobile phone on which you receive one-time passwords, you must change/deregister the phone number as quickly as possible. If you also lose your card, you must block it (see 10).

You must keep your code secret. If you think that someone other than you, knows your code, you must change it at www.nets.eu/3ds.

7 Checking of account entries

You have an obligation to check the entries on your account on a regular basis. If, when checking your account entries, you discover any transactions that do not match your receipts, or that you do not believe you have made, you must contact us as soon as possible. In this connection, be aware of the deadlines stated in clauses 8 and 9.

In connection with the regular checking of your account entries, be aware that when you use your card to make online purchases or purchases by mail order or telephone order, the merchant may generally not debit the amount until the goods have been dispatched. When booking, for example, plane tickets or concert tickets, the merchant will, however, debit the amount already when you book the flight or concert ticket.

8 Reversal of authorised payments

8.1 If you did not know the final amount when authorising a payment
If you did not know the final amount when you authorised a payment, and the amount subsequently debited to your account is considerably higher than you could reasonably expect, you may be entitled to a reversal of the payment. This may, for example, be the case if you hire a car or check out of a hotel, where you have authorised the merchant to debit your card for refuelling the vehicle or restocking the minibar, for example.
If you believe that you are entitled to have a payment for which you did not authorise the final amount reversed, you must contact us no later than eight weeks after the amount was charged to your account.

8.2 Purchases online, by mail order and telephone order, etc.
If you have used your card to buy goods or services

- online
- by mail or telephone order
- in other situations where the card is not read but where card data and the personalised security credentials (for example one-time password, MitID or the like) were used 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 merchant has charged a larger amount to your card account than agreed
- the goods or services ordered have not been delivered
- you exercise your statutory or agreed right of cancellation before the goods or services have been delivered

Before contacting us, you should first try to solve the problem with the merchant. You must be able to document that you have contacted or tried to contact the merchant.

You must submit your dispute to us as soon possible, and, if possible, not later than two weeks after you discovered or should have discovered that one or more amounts had been fraudulently debited to your account. When we assess whether you have

contacted us in due time, we attach importance to your duty to regularly check entries in your account (see 7).

We will subsequently investigate your dispute. While your dispute is being investigated, the disputed amount will normally be credited to your account. If your dispute subsequently proves to be unjustified, we will withdraw the amount from your account.

If we find your dispute unjustified, we are entitled to charge interest from the date on which the amount was deposited in your account to the date on which it was withdrawn. We may also charge a fee for ordering copies of relevant receipts (see the tariff of charges).

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

8.3 Reversing payments made in connection with distance marketing

The situation may differ depending on whether payment was made using your Dankort or Visa card. You can obtain information about this at www.danskebank.dk/indsigelse.

9 Reversal of unauthorised payments

If you believe that your Visa/Dankort card has been used for one or more payments that you have not authorised or made, you must contact us as soon as possible after you become aware of the unauthorised transaction.
When we assess whether you have contacted us in due time, we attach importance to your duty to regularly check entries in your account (see clause 7). In any case, you must contact us within 13 months of the amount having been debited to your account.

We will subsequently investigate your dispute. While your dispute is being investigated, the disputed amount will normally be credited to your account. If your dispute subsequently proves to be unjustified, we will withdraw the amount from your account.

If the investigation shows that there was unauthorised use of the card by other parties, we may hold you liable for this (see clause 11).

If we find your dispute unjustified, we are entitled to charge interest from the date on which the amount was deposited in your account to the date on which it was withdrawn. We may also charge a fee for ordering copies of relevant receipts (see the tariff of charges).

10 Your duty to block your card

Cards

You must contact us as soon as possible to have your card blocked if

- you lose your card
- someone else knows your personalised security credentials, for example your PIN
- you discover unauthorised use of your card
- you suspect that your card has been copied
- you otherwise suspect that there is a risk of unauthorised use of the card

In Danske eBanking and Danske Mobile Banking, you can block your card immediately.

If you do not have Danske eBanking or Danske Mobile Banking, please contact us on tel. +45 70 20 70 20 (open 24 hours a day). When you call, please state your name and address and, if possible, your card and account numbers or CPR number.

When a card has been blocked, you will be informed about why and when the card was blocked.

If you lose your card but find it again, you must contact us to find out what to do.

Please note that if your card is blocked, you cannot use it in wallets.

Cards in wallets

As with the physical card, you must also block your virtual card on your mobile phone if

- you lose your phone
- you become aware of unauthorised use of your virtual card on your mobile phone

- you otherwise suspect that a card in your wallet may have been used without your authorisation.

You can block your card by calling us on tel. +45 70 123 456 (open 24 hours a day). When you call, please state your name and address and, if possible, your card and account numbers or CPR number.

When a virtual card in a digital wallet on your mobile phone has been blocked, you will be informed of why and when the card was blocked.

If your mobile phone with a blocked card is found again, please contact us to agree on what to do.

If someone else finds out the PIN for the digital wallet(s) in which your card is registered, you must change the PIN immediately. Follow the instructions in your digital wallet and contact us for further information about what to do.

11 Your liability in case of unauthorised use

If your Visa/Dankort card has been subject to unauthorised use by another person, Danske Bank covers the loss unless the circumstances of the loss fall within those listed in the clauses below. In such case, Danske Bank has the burden of proof.

In case of unauthorised use of your Visa/Dankort card by another person who has also used your personalised security credentials, you may be liable to pay up to DKK 375 of the total loss.

In case of unauthorised use of more of your cards with the same personalised security credentials (for example the PIN) in connection with the same incident, you may be liable to pay up to a total of DKK 375. It is a condition, however, that you block all cards at the same time. This applies to cards issued by Danske Bank.

You must cover losses up to DKK 8,000 if your Visa/Dankort card has been subject to unauthorised use by another person and your personalised security credentials have been used, and

- you failed to notify us immediately after you discovered that your card or your mobile phone with the card in a digital wallet was lost or that another person had found out your personalised security credentials, or
- you knowingly disclosed your personalised security credentials to the person who used your card without authorisation, while you did not and could not be expected to realise that there was a risk of unauthorised use, or
- you made the card abuse possible through gross negligence

Your total liability cannot exceed DKK 8,000.

Your total liability is limited to DKK 8,000 if two or more of your cards for which you have the same PIN have been used fraudulently in the same incident. However, this requires that all cards with the same PIN are blocked at the same time. This applies to cards issued by Danske Bank.

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

- You willingly gave the personalised security credentials to the person who used your Visa/Dankort card without authorisation
- 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 committed fraud or have deliberately failed to fulfil your obligations under these conditions. Your obligations include keeping your card and mobile phone secure, protecting your personalised security credentials (for example, the PIN) (see clause 4), and blocking your card (see clause 10).

If you have several cards with the same personalised security credentials, the unlimited liability applies to each card that has been subject to unauthorised use.

You are not liable for losses arising after we have been asked to block your card.

Moreover, you are not liable for losses if you are unable to block your card because of conditions for which we are responsible.

You are also not liable if the loss, the theft or the unauthorised acquisition of the personalised security credentials could not be detected by you prior to the unauthorised use.

Furthermore, you are not liable for unauthorised use of the card if this is attributable to actions by Danske Bank's employees, agents or branches or by an entity to which Danske Bank's activities has been outsourced or due to such entity's lack of action.

Danske Bank's liability for your loss is as stipulated in the Danish Payments Act (Lov om betalinger) if the payee knew or should have known that this was a case of unauthorised use of the card.

Danske Bank is also liable as stipulated in the Danish Payments Act if you incur a loss as a consequence of unauthorised use where Danske Bank does not require use of personalised security credentials, unless you have acted fraudulently.

You are liable only for losses resulting from other persons' unauthorised use of the card if the transaction is correctly recorded and entered in the accounts of Danske Bank.

12 Danske Bank's rights and liability

12.1 Danske Bank's notification of unauthorised use and security threats

We contact you if we suspect or discover unauthorised use of the agreement. We also contact you if we become aware of any potential security threats. We contact you in a secure way, for example by sending a message in Danske eBanking, Danske Netpost or e-Boks, by email or by telephone.

12.2 Danske Bank's right to block your Visa/Dankort card

We are entitled to block your Visa/Dankort card if

- your card account is closed, or
- you violate these conditions, or your card account shows an excess, or
- your Visa/Dankort card has been subject to unauthorised use or is suspected of having been subject to unauthorised use by a third party

In case of an excess, we will send you a written reminder before we block your card. Immediate blocking may be necessary, however, if the excess is substantial and/or if you have repeatedly overdrawn your account.

We may also demand that all cards issued for the card account be returned.

When we have blocked your Visa/Dankort card, we will send you a letter stating the reason for and the time of the blocking.

We may contact you by telephone or in another secure way, if we suspect that your card has been used fraudulently or in the event of unauthorised use or security threats.

Note that Danske Bank, merchants, Nets and others will never ask you to state your MitID, PIN or other personal security credentials, such as a password for online purchases or a one-time password received by text message.

12.3 Card replacement

We are entitled to replace your card at any given time.

12.4 Danske Bank's liability

Danske Bank is liable for the tardy or defective performance of its contractual obligations resulting from error or negligence. Even in those areas in which a stricter liability applies, Danske Bank will not be liable for losses arising from:

- breakdown of or lack of access to IT systems or damage to data in these systems due to any of the factors listed below and regardless of whether Danske Bank or a third-party supplier is responsible for the operation of these systems
- power failure or a breakdown of Danske Bank's telecommunications, legislative or administrative

intervention, acts of God, war, revolution, civil unrest, sabotage, terrorism or vandalism (including computer virus attacks or -hacking)
- strikes, lockouts, boycotts or picketing, regardless of whether Danske Bank or its organisation is itself a party to or has started such conflict and regardless of its cause (this also applies if the conflict affects only parts of Danske Bank)
- other circumstances beyond Danske Bank's control

Danske Bank is not exempt from liability if
- Danske Bank ought to have foreseen the cause of the loss when the agreement was concluded or ought to have avoided or overcome the cause of the loss
- under Danish law, Danske Bank is liable for the cause of the loss under any circumstances

12.5 Industrial conflicts
You cannot use your Visa/Dankort card in Denmark if Danske Bank and/or our operational centres are involved in an industrial conflict. You will be informed as soon as possible through the Danish daily press of the beginning and conclusion of such conflict.

You cannot expect to use your Visa/Dankort card outside Denmark if one or more of Danske Bank's operational centres and/or one or more of our international business partners become involved in an industrial conflict. When industrial conflicts occur outside Denmark, you can still use your Visa/Dankort card in Denmark.

12.6 Defective goods or services
Danske Bank is not liable for defective goods or services provided by a merchant. Any complaints concerning defects in the goods or services provided must be addressed to the merchant.

13 Expiry

You may use your card up to and including the month of expiry embossed on the card. On expiry, your card will be invalid.
You will receive a new card before your existing card expires. We may also inform you that you can pick up your new card at one of our branches.

14 Termination

We may terminate the agreement at two months' notice. In the event of termination, you will be reimbursed a proportionate share of any fees that you may have paid in advance for use of the card.

You may terminate the agreement at one month's notice. If you terminate the agreement before the end of the first six months, we may charge a termination fee.

If you or Danske Bank terminates the agreement, you must cut your card in half and throw it away.

15 Changes to the card conditions

We may make changes to these conditions and our fees and charges without notice if the changes are to your advantage. If the changes are not to your advantage, we must give you two months' notice.

We notify you of changes by letter or digital message. You must inform us of any changes in your postal and/or email address. If you fail to do so, you cannot hold us responsible for not having notified you of changes to these card conditions.
Changes to the card conditions will be regarded as having been accepted unless, before the changes take effect, you inform us that you do not wish to be bound by the new conditions.

If you inform Danske Bank that you do not wish to be bound by the new conditions, the agreement will be regarded as having been terminated as from the date on which the new conditions take effect. If you have paid a year's fee in advance, you will be reimbursed a proportionate share of the fee.

16 Complaints

In case of a disagreement on your business relationship with us, you should always contact your branch to make sure that such disagreement is not based on a

misunderstanding. Alternatively, you can call us on tel. +45 33 44 00 00 (open seven days a week).
If you still disagree with or are dissatisfied with the outcome, you must write to our Complaint Management Function, which is in charge of handling customer complaints at Danske Bank.

The address is

Danske Bank
Complaint Management Function
Bernstorffsgade 40
DK-1577 Copenhagen V
Email: klageservice@danskebank.dk

If you are dissatisfied with the outcome, you may submit a complaint to

The Danish Financial Complaint Board
(Det finansielle ankenævn)
Amaliegade 7
DK-1256 Copenhagen K
Tel. +45 35 43 63 33
www.pengeinstitutankenaevnet.dk

You may also submit a complaint to the authorities supervising Danske Bank's compliance with the Danish Payments Act. The Danish Consumer Ombudsman supervises compliance with the duty of disclosure in connection with the provision of payment services, rights and obligations for the use of payment services, use of payment data and information on fees. The Danish Competition and Consumer Authority supervises rules on fees in general.

The Danish Competition and Consumer Authority
(Konkurrence- og Forbrugerstyrelsen)
Carl Jacobsens Vej 35
DK-2500 Valby
www.kfst.dk

If you wish to complain because your card has been blocked, you must contact your branch. If your complaint is rejected, you may complain to the Danish Data Protection Agency at the following address:

The Danish Data Protection Agency
Carl Jacobsens Vej 35
DK-2500 Valby
www.datatilsynet.dk

17 New copies of card conditions

If you need a new copy of these card conditions, you can find them at www.danskebank.dk. You are also welcome to contact us.

18 Fees and currency conversion

18.1 Danske Bank's fees and charges

Any fees are specified at www.danskebank.dk. It is also stated when they are charged and whether or not they are charged in advance.

18.2 The merchant's fees

When you use your Visa/Dankort card abroad or to make online purchases from a merchant abroad, the merchant may charge a fee.

18.3 Exchange rates

Purchases made outside Denmark are translated into Danish kroner and are always payable in Danish kroner.

Conversion of foreign currencies to Danish kroner is based on an average rate calculated on the basis of Visa exchange rates for all transactions on that day in the same currency. See the Visa exchange rates at www.nets.eu/valutakurser (website available in Danish only).

Exchange rates change continually and without notice.

An exchange rate may change from the time you use your card until the amount is charged to your card account.

There is a charge for foreign card payments outside the EU/EEA, Switzerland, UK, Greenland, Faroe Islands, Andorra, Monaco, San Marino and Vatican City

When you have used your card for a purchase or to withdraw cash in an EEA currency other than Danish kroner you will receive a text message from Danske Bank informing you of our charge for the card payment.

The text message is sent the first time you make a payment in an EEA currency and subsequently at least

once a month if you use the card for payments in an EEA currency.

You can unsubscribe from text messages by sending a text message with the text "STOPCCY" to 3326. We will then no longer send the text messages.

You pay any costs related to internet and mobile data use when we send you text messages.

18.4 Currency conversion by merchants abroad (Dynamic Currency Conversion)
If you use your card abroad, the merchant may offer to convert the amount into Danish kroner before the payment transaction is processed. Before you accept this conversion, the merchant must inform you of any fees and the exchange rate that will be used for the conversion.

You should be aware that the exchange rate that the merchant uses may differ from the exchange rate that we use, and that we do not have any influence on the exchange rate used by the merchant.

19 Credit assessment

We will assess your financial position before issuing a Visa/Dankort card to you.

20 Consent to using, retaining and disclosing data
On acceptance of these conditions and use of the Visa/Dankort card, you consent to our processing your personal data. When you use the card, we consider the card number, amount, date of use and location of use etc. to be personal data.

Processing of information about you is done solely for purposes necessary for you to use the card as agreed, including completion of transactions. The data is processed in accordance with applicable data protection legislation, including the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council).

The data is retained by the merchant, the merchant's bank and the bank's data supplier (for example Nets) and retained by us for bookkeeping, account specifications and any subsequent correction of errors. When you use the Visa part of your Visa/Dankort card, data for processing your payment will also be retained by Visa Inc. Visa Inc. is obligated to retain and process the data in accordance with the European Union's General Data Protection Regulation.

Data is disclosed only for processing of transactions when required by law or to prevent unauthorised use of the card. The data is retained for the current year plus the following five years.

When you register for Dankort Secured by Nets and Visa Secure, your mobile phone number will be disclosed to and retained by Nets in order for Nets to be able to send you one-time passwords.

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

If you are dissatisfied with our processing of your personal data, you may submit a complaint to

Danske Bank
Complaint Management Function
Bernstorffsgade 40
DK-1577 Copenhagen V
Email: klageservice@danskebank.dk

or to

The Danish Data Protection Agency
Carl Jacobsens Vej 35
DK-2500 Valby
www.datatilsynet.dk

21 Supervision

Danske Bank is subject to supervision by the Danish Financial Supervisory Authority and is registered in

the Danish Financial Supervisory Authority's register with registration number 3000.

22 Definitions

Business day: A business day is a weekday. Saturdays, Sundays, public holidays, Friday after Ascension Day, 5 June, 24 December and 31 December are not business days.

Dankort Secured by Nets: Dankort Secured by Nets is a solution that offers extra protection of customer data in online transactions.
Digital wallet: A digital wallet is a personal software-based solution in which you register your card details for use in connection with future online purchases from a merchant.

Dynamic currency conversion: Used by some merchants so that you can pay in Danish kroner abroad. The merchant performs the currency conversion, and we have no influence on the exchange rate used.

One-time password: A password that you receive by text message on the registered mobile phone. You must use the password for online purchases at merchants using the Dankort Secured by Nets or Visa Secure solution.

Single PIN: The same personal and secret PIN linked to several cards.

Loyalty programmes: Loyalty programmes is a collective term used for solutions in which you can register your card with a provider of a loyalty programme and subsequently, when using the card, earn bonus points, etc. or contribute to a charitable cause.

Merchant: All shops, hotels, restaurants or other outlets accepting Dankort and/or Visa cards.

Contactless payment: Contactless payment is payment using the card chip without having to insert the card into the terminal.

Card: The physical card

Receipt: A statement on paper or in digital form specifying the details of a payment.

MitID: MitID is a digital signature you can use to register for Dankort Secured by Nets and Visa Secure.

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

Personalised security credentials
Personalised elements made available to you as the cardholder in order to authenticate you. Personalised security credentials may be a PIN, a code for a digital wallet, a fingerprint, face recognition or the like. Dankort Secured by Nets and Visa Secure are considered to be personalised security credentials.
PIN: The personal and secret number that is linked to your card.

Tariff of charges: The list of fees and other charges applicable at any given time. You may obtain a copy of the tariff of charges from Danske Bank's branches.

Exchange rate: An exchange rate used for translating payments in foreign currency into Danish kroner.

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

Transaction: A cash withdrawal or a single purchase in a physical store, online shop or the like.

Unique device ID:
Unique device ID is used in payment software which is security-approved according to the PCI standard and in which you may store parts of your card information.

When you want to pay in an online shop, you can retrieve saved card data so that you are required to enter only the card validation code (CVC/CVV) on the back of your payment card to authorise the transaction.

Visa Secure: Visa Secure is a solution offering added protection of customer data in online transactions.

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

Visa/Dankort card: A collective term for the physical card bearing the Visa and Dankort logos.

Wallet provider: A provider of a wallet.

Wallet: A personal software-based solution allowing you to store a virtual version of your card. The wallet is an app you can download to your mobile phone.

Danske Bank A/S
CVR-nr. 61 12 62 28 - København

The Danish Payments Act

Liability rules

97. Disputes relating to unauthorised or incorrectly executed payment transactions must be received by the provider as soon as possible and not later than 13 months after the debit date of the relevant payment transaction. The deadline is calculated from the time at which the provider has communicated this information or made it available, if it has not been communicated in advance.

(2) Disputes relating to unauthorised or erroneous payment transactions initiated via a provider of payment initiation services, must be addressed to the account-holding provider in accordance with subsection (1), see, however, section 99(2) and (3) and section 104.

98. If a payer denies having authorised or initiated a payment transaction, the provider of the payment service must prove that the payment transaction was correctly registered and booked and not affected by technical failure or other errors, see, however, subsection (3). In connection with the use of a payment instrument, the provider furthermore has to prove that the payment instrument's personalised security feature was used in connection with the payment transaction.

(2) If a payer denies having authorised or initiated a payment transaction, the recorded use of a payment instrument is not in itself proof that the payer authorised the transaction, that the payer acted fraudulently or failed to fulfil his obligations.

(3) If a payer denies having authorised or initiated a payment transaction which was initiated via a provider of payment initiation services, the provider of the payment initiation service must prove that the payment transaction was correctly registered and booked and has not been affected by technical failure or other errors.

100. The payer's provider of payment services is liable to the payer for any loss incurred due to the unauthorised use by a third party of a payment service unless otherwise provided in subsections (2) to (5) hereof. The payer is only liable under subsections (3) to (5) hereof if the transaction was accurately recorded and entered in the accounts, see, however, subsection (2).

(2) However, the payer is liable without limitation with respect to any loss incurred due to the payer acting fraudulently or wilfully failing to fulfil his obligations under section 93.

(3) Except where subsections (4) and (5) hereof provide for more extensive liability, the payer is liable for an amount up to DKK 375 for any loss incurred as a result of the unauthorised use by a third party of the payment service where the personalised security feature linked to the payment service has been used.

(4) Except where subsection (5) provides for more extensive liability, the payer is liable for an amount up to DKK 8,000.00 for any loss incurred as a result of the unauthorised use by a third party of the payment instrument if the payer's provider is able to establish that the personalised security feature linked to the payment instrument was used; and

1) that the payer failed to notify the payer's provider as soon as possible after having become aware that the payment service's payment instrument was missing or that the personalised security feature linked to the payment instrument had come to the knowledge of an unauthorised user;

2) that the payer intentionally made the personalised security feature of the payment instrument available to the person making such unauthorised use without this falling within the scope of subsection (5); or

3) that, through grossly inappropriate conduct, the payer made such unauthorised use possible.

(5) The payer is liable without limitation with respect to any loss incurred due to the unauthorised use by a third party of the payment service where the personalised security feature linked to the payment instrument was used and the payer's provider proves that the payer disclosed the personalised security feature to the person making the unauthorised use, and that the circumstances were such that the payer knew or ought to have known that there was a risk of abuse.

(6) Notwithstanding the provisions of subsections (3) to (5) hereof, the payer's provider is liable for any unauthorised use

1) after the provider was notified that the payment instrument linked to the payment service had been lost, that the personalised security feature had come to the knowledge of an unauthorised person, or that the payer required the payment instrument to be blocked for any other reason;

2) when it is caused by actions taken by a service provider's employees, agents or branch or an entity to whom the service provider's activities have been outsourced, or their passivity; or

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

(7) Notwithstanding subsections (3) to (5) hereof, the payer's provider is also liable, unless the payer has acted fraudulently. The payment recipient or his/her provider must compensate the loss suffered by the payer's provider if the payee or its service provider has failed to use strong customer authentication. Subsections (1) and (2) do not apply to the services comprised by section 1(5) and section 5(14)-(16).

(8) Notwithstanding the provisions of subsections (3) to (5) hereof, the payer's provider is also liable if the loss, theft or unauthorised acquisition of the payment instrument linked to the payment service or the personalised security feature linked to the payment service could not be detected by the payer prior to the unauthorised use.

(9) Moreover, notwithstanding the provisions of subsections (3) to (5) hereof, the payer's provider is liable if the payee knew or ought to have known that the use of the payment service was unauthorised.

(10) The provisions of subsections (1) to (9) hereof also apply to electronic money except where the payer's provider of electronic money is unable to block the payment account or the payment instrument.