

CARD CONDITIONS VISA/DANKORT

Effective from 1 January 2018

Below we set out the conditions that apply to Visa/Dankort cards.

1 Visa/Dankort card conditions

These conditions apply to the use of Visa/Dankort cards. They describe the use of the card as a Dankort card and as a Visa card, both as physical cards and the Dankort card linked to your mobile phone. Unless otherwise specified, the conditions apply to both Dankort and Visa cards as physical cards and Dankort on your mobile phone. Definitions of terms used are listed at the end of this document.

2 Use

A Visa/Dankort card is a payment instrument that you may use 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. You may overrule the merchant's choice where technically possible in accordance with the legislation in force.

The entries in your account specify whether a payment has been completed as a Dankort or a Visa transaction.

Please note that Visa card payments may be subject to fees and charges, and that the transaction amount is included in the monthly spending limit on your Visa card, see clause 2.5.

2.1 Cash withdrawals

You may use your Dankort card to withdraw cash from ATMs in Denmark. You may also use your card to withdraw cash at Danske Bank's branches and at most other banks in Denmark.

Please note that not all ATMs accept the Dankort card. If so, the withdrawal is handled as a Visa card transaction.

Visa card fees are stated in the list of charges.

2.2 Purchases

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 use your card to make online purchases as well as purchases by mail order and telephone order. You may also use your Visa/Dankort 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.

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

In connection with Visa card purchases abroad, you may be asked to choose whether

the purchase should be made in the local currency or in Danish kroner, see clause 17.3 for further details.

2.3 Account transfers via Danske Bank ATMs

You may use your card to make transfers via our ATMs to Danske Bank accounts and to accounts held with other banks in Denmark.

2.4 Charges to your card account

As a general rule, purchases and cash withdrawals made using your Dankort card are debited to your account on the day you make the purchase or cash withdrawal. Visa card transactions are entered the day after the purchase or cash withdrawal at the earliest. The time at which the amount is debited to your account depends, however, on when we receive the transaction.

2.5 Spending limit

Unless otherwise agreed, purchases and cash withdrawals may not exceed the current balance in your account.

Contactless function or Dankort on your mobile phone

If you use the contactless function or Dankort on your mobile phone, an amount limit applies to each transaction without entering your PIN. The list of charges specifies this limit.

Gambling and lottery

When you use your Dankort card at outlets providing gambling and betting services – that is, when you use your card at casinos, for buying lottery tickets, on race courses, etc. – it may be subject to a daily spending limit. The list of charges specifies this limit.

Cash withdrawals

Your Dankort card is subject to a limit on cash withdrawals per day. The amount is stated in the list of fees and charges.

Your Visa card is subject to an overall limit on purchases and cash withdrawals over a 30-day period. Limits also apply to the total amount of cash that you may withdraw at banks and from ATMs every day. The list of charges specifies these limits.

Other

Merchants may set their own purchase limits, while banks may set their own limits on cash withdrawals.

You may have to pay a fee every time you withdraw cash regardless of the amount withdrawn.

2.6 Card with spending limit

You can allow your child or others to pay with your Visa/Dankort card subject to specific restrictions.

This is done by setting up your Visa/Dankort card in a mobile phone app and then setting spending limits. When you have set up the card, the person in question can use his or her mobile phone to pay for purchases at merchants.

2.7 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 that have been approved by Nets. Go to this website to see the loyalty programmes that have been approved: dankort.dk/Pages/Loyalitetskort.aspx.

3 Visa/Dankort card use

Before you authorise a payment or cash withdrawal, you must always check that the amount is correct (look at the terminal or the receipt, for example). Generally, you cannot revoke transactions already authorised (see clauses 8 and 9 for exceptions).

You should always get a receipt for a payment or cash withdrawal. 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 to check that the correct amount is debited to your account (see clause 7). At self-service machines, you may not get a receipt.

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

When the data is read digitally directly from your Visa/Dankort card by using

- the chip or magnetic strip and PIN
- the chip or magnetic strip and signature
- the contactless payment function
- the wallet - for instance Dankort on your mobile phone
- the chip or magnetic strip but not the PIN at self-service machines

When the data is not read digitally from your Visa/Dankort (for instance for online transactions) by using the card number, expiry date and card validation code

When card data has been registered in advance, for instance

- agreements with individual merchants to register card data for use in connection with future purchases approved and initiated by you

- subscriptions under which the merchant draws 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 purchases approved 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) on 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 to which you have given your consent.

3.1 Contactless function

If your card has the contactless function, you can use this function to make purchases at merchants offering that service. Payment is made without inserting the card in a terminal. Instead, you accept the payment by holding the card within 0-3 centimetres of a terminal with an active contactless payment function.

Terminals with a contactless payment function bear the following symbol:



An amount limit applies to each transaction made without entering your PIN, see clause 2.4 (the current limit is DKK 350). [Name of bank] may adjust the amount. You will not receive any notice of adjustments, unless the amount is increased or reduced by more than 50% within a calendar year. Information about the current limit is always available at danskebank.dk.

If the amount of the transaction exceeds the current limit, you will automatically be asked to authorise the payment by entering your PIN.

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

3.2 Wallets

If you already have a physical Visa/Dankort card, your Dankort card can be linked to your mobile phone. This function is called Dankort on your mobile phone. First, you must download an approved wallet for Dankort on your mobile phone. You can see a list of approved wallets on dankort.dk/Pages/Dankort-i-apps.aspx. You can register in all approved wallets that have opened up for Dankort on your mobile phone from us. Registration takes place by use of NemID (or similar security). There may be limits to how many times you can link the physical Dankort card to your mobile phone.

During the registration process, you must select to which physical card you want to link the Dankort on your mobile phone. In addition, you will be asked to choose a personal PIN, which you must use if a purchase with Dankort on your mobile phone requires that you enter a PIN. Follow the instructions in your wallet.

You cannot use Dankort on your mobile phone for purchases online, by mail order and telephone order.

3.3 Self-service machines without PIN

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

3.4 Using card number, expiry date and card validation code

You must enter the card number, expiry date and card validation code to trade online.

If you use your Visa card to trade online with a Verified by Visa merchant, you also need to enter the one-time password you receive by text message from Nets.

If you use your Dankort card and the merchant is registered with Dankort Secured by Nets, you may also be asked to enter the one-time password that you receive by text message

from Nets in connection with the purchase, see clause 6.

To make purchases by mail or telephone order, you must state the card number, expiry date, card validation code and, if required, name and address. When you make a purchase by mail order, you must also sign the order form. Never disclose your PIN in any of the above transactions.

You cannot use Dankort on your mobile phone for purchases online, by mail order and telephone order.

3.5 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 do not have to enter your card data when approving future online purchases. You must follow the instructions provided by the merchant or the wallet provider.

Go to dankort.dk/Pages/Dankort-i-apps.aspx to see which wallet providers have been approved

and with which you can sign up the Dankort part of your Visa/Dankort.

You can also agree with the merchant that your card data is registered with the merchant for the payment of a subscription. The merchant automatically withdraws the agreed subscription payments so you do not have to approve each individual subscription payment. When using your card data in this way, make sure that any cancellation of subscriptions is made in accordance with the terms and conditions stipulated by the merchant.

It applies to all the solutions described in this paragraph 3.5 that, if you get a new card, you must contact the merchant or the provider of the digital wallet solution yourself in order to register the new card data.

4 Protection of your Visa/Dankort and PIN

Card

Your card is personal and may be used only by you. Upon receipt of the card, you must sign the signature field on the back of the card. You

may not hand over or give the card to other persons.

This also applies to Dankort on your mobile phone, see, however, Dankort on your mobile phone with spending limit.

PIN

Your PIN is personal and may be used only by you. You automatically receive a PIN for your card. When you receive your PIN, you must check whether others may have had access to it. If you suspect this, you must contact us immediately.

Memorise your PIN and subsequently destroy the letter. Do not keep your PIN with your card or write it on your card. Also do not save the PIN in or together with your mobile phone.

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

If you suspect that others have gained access to your PIN, you must contact us immediately and at the same time change the PIN to the Dankort card on your mobile phone.

If you are unable to memorise your PIN or want to keep evidence of it, you must store it in a safe place. If you need to write down your PIN, use the PIN memoriser that you have received from us or get one from your branch.

5 Authorisation to use your account

If you want another person to be able to use your account for Visa/Dankort transactions, this person must have his or her own personal card and PIN. The cardholder is subject to the same conditions as those you must observe.

However, special conditions apply to Dankort on your mobile phone with spending limit. See clause 2.6

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

6 Secure online payments

Dankort Secured by Nets and Verified by Visa offer extra protection against unauthorised use of card data in connection with online purchases. When you shop online, you must enter a one-time password after having entered your card details. You receive the one-time password by text message from Nets when you are making the payment.

You will also be able to use your NemID for Verified by Visa and Dankort Secured by Nets. For example, if you have not informed us of your mobile number or if you have changed your mobile number, see section 6.1.

6.1 How to register

When you receive your new card, it will automatically be registered with Verified by Visa and Dankort Secured by Nets if we have your mobile number on file. We disclose your mobile number to Nets in order for Nets to be able to send you one-time passwords.

If you change your mobile number, please update your information on danskebank.dk/betal-sikkert. If we do not have your mobile number on file, you can complete your transactions using NemID. You can also register your mobile number with Nets using your NemID to receive the one-time password you need to complete the transaction.

Note that not all Dankort card transactions require Dankort Secured by Nets even though the merchant indicates that it uses this feature. Minor transactions can often be concluded without the use of Dankort Secured by Nets.

6.2 Security - cards and telephone

Since your mobile phone becomes an element of the added protection offered by Verified by Visa, 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 with Verified by Visa as quickly as possible. If you also lose your card, you must block it (see clause 10).

7 Account entries

You must regularly check the entries in your account. If you discover entries that do not match the information on your receipts or that you do not believe you have made, you must contact us as soon as possible. See clauses 8 and 9 for more information on deadlines for revoking transactions.

Merchants may generally not charge online purchases or purchases by mail or telephone order to your account until the goods have been sent. But if you book flight or concert tickets, for example, the merchant may charge the amount to your account at the time of booking.

8 Reversal of authorised payments

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

If you did not know the final amount when you authorised a payment and the amount charged to your account is considerably higher than you could reasonably expect, you may be entitled to revoke the payment. This may be the case if, for example, you rented a car or stayed at a hotel and allowed the merchant to subsequently charge petrol or mini-bar purchases to your account.

If you believe that you are entitled to revoke a payment, you must contact us no later than eight weeks after the amount was charged to your account.

8.2 Online use etc.

If you have used your card to buy goods or services

- online
- by mail or telephone order
- in other situations in which you cannot present your card but must provide card data

(the card number, for example) to complete the transaction

- at self-service machines where your PIN is not required

you may be entitled to revoke the payment 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 always try to settle the matter with the merchant having charged the amount. 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 clause 7).

We will subsequently investigate the matter. Normally, we will deposit the amount in your card account. If we find your objection unjustified, we will withdraw the amount from your account.

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

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

8.3 Revoking payments made in connection with distance marketing (such as online shopping)

The situation may differ depending on whether payment was made with your Dankort or Visa

card. For more information, see danskebank.dk/carddispute.

9 Reversal of unauthorised payments

If you believe that your Visa/Dankort has been used for one or more unauthorised payments, you must contact us as soon as possible.

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). We must receive your objection within 13 months of the amount having been charged to your account.

We will subsequently investigate the matter. Normally, we will deposit the amount in your card account. If we find your objection unjustified, we will withdraw the amount from your account.

If our investigation shows that another person has fraudulently used your card, we may hold you liable in accordance with the rules specified in 11.

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

10 Duty to block your card

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

- you lose your card
- another person finds out your PIN
- you discover unauthorised use of your card
- you suspect that your card has been copied
- you suspect potential unauthorised use of your 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, you should contact us on tel. +45 70 20 70 20 (open 24 hours a day). When you call, state your name and address

and, if possible, your card and account number or CPR number.

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

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

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

- you lose your mobile phone
- you find out that a card in your wallet has been used without your authorisation
- 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, state your name and address and, if

possible, your card and account number or CPR number.

When the Dankort card on your mobile phone has been blocked, you are informed about why and when the card was blocked.

If a mobile phone with a blocked Dankort card is found again, you must contact us so that we can agree what you should do.

If another person learns the PIN to the Dankort card on your mobile phone, you must change it as soon as possible. Follow the instructions in the wallet. Then contact us for further information about what you should 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 clause 11. In such cases, Danske Bank has the burden of proof.

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

Your total liability is limited to DKK 375 if two or more of your cards for which you have a single PIN are used fraudulently in the same incident. It is a condition, however, that you block all cards issued by Danske Bank at the same time.

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

- you failed to notify us immediately after you discovered that your card or your mobile phone with the card in a wallet was lost or that another person had found out your PIN, or
- you disclosed your PIN to the person who fraudulently used your card, while you did not and could not be expected to realise that there was a risk of unauthorised use, or

- you made unauthorised use of your card possible through gross negligence

You must cover losses up to DKK 8,000 if your card has been subject to unauthorised use by another person through physical or electronic reading and your signature has been forged by this person, and

- you or any person to whom you had given your card failed to notify us as soon as possible after you or the person in question discovered that the card was lost, or
- you or any person to whom you had given your card made unauthorised use of the card 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 a single PIN have been used fraudulently in the same incident. It is a condition, however, that you block all cards with the same PIN issued by Danske Bank at the same time.

You are liable for the full loss if your PIN has been entered in connection with the unauthorised use and you disclosed your PIN to the person who fraudulently used your Visa/Dankort, and you realised or were expected to realise 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 the rules. These obligations include keeping your card and mobile phone safe, protecting your PIN and blocking your card (see clause 10).

If you have two or more cards with a single PIN, the unlimited liability applies to each card used fraudulently.

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 personal security solution could not be detected by you prior to the unauthorised use.

12 Danske Bank's rights and liability

12.1 Notification to you in case 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 safe way, for example by sending a message in Danske eBanking, Danske Netpost, e-Boks, by email or by telephone.

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

We are entitled to block your Visa/Dankort if

- your card account is closed
- you violate these conditions, or your card account shows an excess
- your Visa/Dankort has been used fraudulently or you suspect unauthorised use by a third party

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

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

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

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

12.3 Card replacement

We are entitled to replace your card at any 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 areas of increased liability, Danske Bank is not 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 part 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 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 outside Denmark if one or more of the bank's operational centres and/or one or more of the bank's international business partners become involved in an industrial conflict. When industrial conflicts occur outside Denmark, you can still use your Visa/Dankort in Denmark.

12.6 Defective goods or services

Danske Bank is not liable for defective goods or services provided by a merchant. Complaints about defective goods or services provided must be made to the merchant.

13 Expiry

You may use your card until the expiry date stated on the card. On expiry, your card becomes invalid. Dankort on your mobile phone expires at the same time as the card to which it is linked.

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. If your agreement is terminated, you receive a proportionate reimbursement of any fees paid in advance for 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 return your card to us. If you return the card to us by mail, remember to cut it in halves.

15 Changes to card conditions

We may change the conditions and charges without giving notice if the changes are to your advantage. If the changes are not to your advantage, we 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 e-mail address. If you fail to do so, you cannot hold us responsible for not having notified you of changes to these card conditions.

When we change the conditions, you must inform us - before the changes take effect - if you do not want to be bound by the new conditions. If we do not hear from you, you will be bound by the new conditions.

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

16 Complaints

You should always contact your branch in case of a disagreement on a business matter. Alternatively, you can call us on tel. +45 33 44 00 00 (open seven days a week). In this way, we make sure that such disagreement is not based on a misunderstanding.

If you still disagree or are not satisfied with the outcome of your complaint, you may contact Danske Bank's Legal department, which is in charge of handling customer complaints.

The address is

Danske Bank
Legal department
Holmens Kanal 2-12
DK-1092 København K

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

Pengeinstitutankenævnet (The Danish Complaint Board of Banking Services)
Store Kongensgade 62, 2. sal
DK-1264 København K
Tel. +45 35 43 63 33
pengeinstitutankenævnet.dk

or

The Danish Consumer Ombudsman
(The National Consumer Agency of Denmark)
Carl Jacobsensvej 35
DK-2500 Valby
Forbrugerombudsmanden@kfst.dk

If you want to complain because your card has been blocked, you must contact your branch. If

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

Datatilsynet
(The Danish Data Protection Agency)
Borgergade 28, 5. sal
DK-1300 København K

17 New copies of card conditions

If you lose this copy of the card conditions or otherwise need a new copy, you can find it at danskebank.dk. You can also contact your branch.

18 Fees and currency conversion

18.1 Danske Bank's fees

Fees charged, if any, are stated in the list of fees available at danskebank.dk. The list also states when fees are charged and whether fees are charged in advance.

18.2 The merchant's fees

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

18.3 Exchange rates

Purchases and cash withdrawals made abroad are converted into Danish kroner, see the list of fees and charges. The amount is always debited to your account in Danish kroner.

In connection with currency conversion, the methods described in the list of charges, see the 'reference exchange rate' paragraph in the list of charges, apply. Changes in the reference exchange rate stated in the list of charges take effect without notice.

An exchange rate may change from the time you use your Visa/Dankort until the amount is charged to your account. Some countries, mainly outside Europe, may operate with several official exchange rates, depending on the source of the exchange rate.

18.4 Dynamic currency conversion

If you use your card outside Denmark, the merchant may propose, before processing the payment, to convert the amount into Danish kroner. Before you accept this conversion, the merchant must inform you of any fees and the applicable exchange rate.

The exchange rate used by the merchant may differ from the one used by us, and we have no influence on the exchange rate used by the merchant.

19 Credit assessment

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

20 Registration of blocked Visa/Dankort

If your Visa/Dankort is blocked (see clauses 10 and 12), your card number is included in the Danish banking sector's register of blocked Dankort and Visa/Dankort cards. Blocked Visa/Dankort may also appear on Visa's list of blocked cards.

The joint register of Dankort cards is available to banks and merchants accepting Visa/Dankort and allows them to check whether cards used for payment transactions are blocked.

21 Supervision

The Danish Financial Supervisory Authority has registered Danske Bank's license under FSA No. 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 on your mobile phone: A virtual version of the Dankort part of your Visa/Dankort card that can be linked to a wallet on your mobile phone.

Dankort on your mobile phone with spending limit: Dankort on your mobile phone with a

spending limit solution under which the cardholder links a spending limit to a virtual card and gives someone else (typically a child) access to use the virtual card within the limit. The cardholder sets the limit for use of the virtual card. A maximum limit for use set by Dankort (Nets) always applies. For payment purposes, the virtual card with a spending limit works in the same way as the Dankort on your mobile phone.

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: Some merchants offer dynamic currency conversion, which allows you to make transactions in Danish kroner outside Denmark. The individual

merchant is responsible for the currency conversion, and we have no influence on the exchange rate used for translation.

One-time password: A password you receive by text message on the mobile phone number you have registered. You must use the password to trade with online merchants using the Verified by Visa solution.

Single PIN: A four-digit personal identification number for two or more cards.

Loyalty programmes: Loyalty programmes is a collective term used for solutions in which the card holder can register his 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 Visa cards.

Contactless payment: Contactless payment is payment using the card chip without having to

insert the card into the terminal. You can simply hold the card within 0-3 centimetres of the contactless payment symbol on the card terminal to make a payment.

Card: The physical card

Receipt: A statement on paper or in electronic form specifying the details of a payment for goods or services provided.

NemID: NemID is a digital signature. We distinguish between Bank NemID and OCES NemID, but you can use both to register for Verified by Visa.

Nets Denmark A/S: Nets Denmark A/S is the company in charge of operating the Dankort system on behalf of the Danish banks.

PIN: The four-digit personal identification number for your physical cards as well as the confidential personal code you have chosen for the Dankort on your mobile phone.

List of charges: Our current list of charges etc. is available from our branches.

Reference exchange rate: An exchange rate used for translating non-Danish payments into Danish kroner.

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

Transaction: a cash withdrawal or a single purchase in an online shop or similar.

Verified by Visa: Verified by Visa is a solution offering extra protection of customer data in online transactions.

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

Visa/Dankort: A collective term used for the physical card and Dankort on your mobile phone.

Wallet provider: A provider of a wallet for use for Dankort on your mobile phone.

Wallet: A personal software-based solution where Dankort on your mobile phone is stored. The wallet is an app you can download to your mobile phone.

The Danish Act on Payments

Liability rules

97. Objections 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) Objections against 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 (3).

(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.