

The signed agreement is to be sent to:

DNB Bank ASA
PO Box 1600 Sentrum
0021 OSLO

Customer information

Organisation number	
Company name	
Postal address	
Postcode and place	

Cardholder information (cardholder must have verified his/her identity in the bank)

Name of cardholder	
Norwegian national identity number (11 digits)	
Address (private)	
Postcode and place	

Card information

Account number	
Card usage options	Payments and withdrawals in Norway and internationally

Amount limits and terms and conditions

Withdrawals from ATMs (cash machines) displaying the VISA sign per 24 hours	NOK 9 900
Withdrawals from banks displaying the VISA sign	Up to available amount in account
Purchase of goods and services/use of point of sale (POS) payment terminals	Up to available amount in account

Signatures

Cardholder	I have read and understood, and accept, the terms and conditions set out on the following pages concerning my liability to the bank in connection with the use of the card.
Date	Signature Name in block letters:

Customer	I/we accept that the above-mentioned person will be issued with this card, which is linked to the company's account. I/we have read and understood, and accept, the terms and conditions set out on the following pages concerning my/our liability to the bank in connection with the use of the card. Signature in accordance with valid certificate of registration.
Place and date	Signature(s) Name in block letters:

For the bank	The bank's departmental stamp and signature as confirmation that the customer and cardholder have given their binding signatures on the agreement, and that signature samples and proof of identity have been obtained and checked.
Date	Department: Signature



Terms and conditions for payment cards and other card-based payment instruments (debit) - corporate customers

Part E of the account agreement

Contents

1. Brief description of the services
2. Establishing a payment card agreement
3. Terms and conditions and information
4. Prices and pricing information
5. Issuing payment cards and personal security information
6. The payment card's validity period and renewal
7. Protection of the payment card and personal security information and reporting lost cards
8. Using the payment card
9. Debit limits, etc.
10. Debits
11. Reservation
12. Retroactive debit
13. Payment order cancellation
14. Receipt and own control
15. Overdrafts
16. Liability in the event of unauthorised use
17. Claims and refunds
18. The bank's blocking of the payment card for security reasons, etc.
19. Technical failure, posting errors or similar
20. The bank's processing of personal data
21. Termination

1. Brief description of the services

The service grants the account holder access to payment cards and other card-based payment instruments issued by the bank, that can be used for payment of goods and services, cash withdrawal and, if the bank offers it, making cash deposits, as well as for other uses as may be specified, with direct debit or credit of the account to which the payment instruments are linked.

In this context, payment cards can be payment cards and other card-based payment instruments, such as virtual cards and procedures that make it possible to use payment cards in mobile phone applications, smartwatches or other digital equipment.

Payment cards have different characteristics and specified areas of use, cf. section 3 Terms and conditions and information and section 8 Using the payment card. The cardholder must normally confirm the payment with personal security information. In some situations, a payment card can also be used without personal security information. Personal security information includes, among other things, personal codes, PIN, fingerprints and facial recognition.

The account holder must follow the applicable rules and instructions from the bank on the use of the payment cards.

Upon agreement with the bank, the account holder may give certain people (e.g. employees) access to the account through the use of payment cards.

These terms and conditions apply both to Visa Business and BankAxept corporate cards, to the extent that they are appropriate for the cards' respective functionality.

A Visa Business corporate card is an international payment card that can be used for purchases of goods and services in payment terminals at Visa merchants, on the internet (online payment), by mail order or phone order or in an application (app) on mobile devices, or to withdraw cash at Visa-branded banks and ATMs (cash machines) internationally, and in other areas of use as specified.

A BankAxept corporate card is a national payment card that can be used in terminals to pay for goods and services (payment terminals), to withdraw cash in ATMs in Norway and within other areas of use as specified. The payment card can also be used as a deposit card or a combined deposit and payment/cash withdrawal card.

2. Establishing a payment card agreement

The agreement is between the bank and the account holder. The account gives the named user of the payment card (hereafter referred to as 'the cardholder') authorisation to access the account through the use of the payment card. Payment instruments can be issued to additional cardholders under this agreement, and by signing the terms and conditions the cardholder makes a commitment to comply with them as far as applicable.

The agreement can be terminated by the account holder or any other person authorised by the account holder to administer the agreement, e.g. via the customer's online bank. Individual cardholders can cancel their payment cards themselves.

Prior to issuing a payment card to a cardholder, the cardholder must state his/her full name, address, Norwegian national identity number or temporary identification number (D number), provide proof of identity and confirm that the information is correct. Normally, such verification of identity and proof of identity must be done through a personal visit by the cardholder to the bank or the bank's representative. The identity and proof of identity of the user in question can also be verified via the cardholder's existing customer/account relationship with the bank. The control is carried out in accordance with the Norwegian anti-money laundering legislation.

The bank will notify the account holder of use of the payment card and changes to the agreement, and the account holder has a duty to inform the cardholder. When the bank notifies the account holder, a letter to his/her last known address is always considered sufficient. If the account holder is an online bank customer, such notifications will only be sent via the online bank.

3. Terms and conditions and information

These terms and conditions are supplemented by the bank's General Terms and Conditions for Deposit and Payment Services. In the event of any inconsistencies, these terms and conditions take precedence over the General Terms and Conditions for Deposit and Payment Services.

In the information received by the account holder, the account holder and cardholder should particularly note:

- a) the payment card's areas of use
- b) the situations in which the payment instrument may be used without a personal code or other personal security information or signature, and the charges that may be debited the account holder's account as a result of such use
- c) how the account holder should prove his/her identity when using the payment card in the different areas of use
- d) safekeeping of the payment card, personal code or other personal security information, and/or mobile device to which the payment card is linked, and advice regarding codes to avoid
- e) the withdrawal and debit limits set out for the payment card's area(s) of use
- f) how to report lost or stolen payment cards and/or personal codes/security information and/or mobile devices linked to the payment card, and how to block the payment card when this happens
- g) the extent to which merchants have the opportunity to reserve amounts in the account in connection with the purchase of goods or services
- h) the account holder's/cardholder's liability and risk in the event of unauthorised payment transactions

4. Prices and pricing information

The costs of establishing, owning and using the payment card are specified in the bank's current price list or the account information and/or are communicated by other appropriate means.

When using the payment card in currencies other than Norwegian kroner, the transaction amount on the sales invoice or withdrawal receipt will be converted from the foreign currency in question to NOK on the same day the amount is settled between the foreign bank and the account holder's bank. The settlement date depends on how quickly the foreign merchant, or its bank connection, sends the payment transaction for settlement. The market exchange rate for the purchase/sale of currency plus a conversion fee is used in the conversion.

5. Issuing payment cards and personal security information

The bank will issue the payment card for use in, e.g., payment terminals, ATMs and other payment solutions. The payment card will be sent to the cardholder or the address specified in the agreement. The cardholder must sign the payment card as soon as it is received. The payment card may also be activated on first use.

The payment card is issued with the cardholder's name and the account holder's account number imprinted. The cardholder will be assigned a personal code and/or other personal security information. The payment card and code are personal and only to be used by the cardholder. The bank must have satisfactory procedures in place for issuing/delivering the payment card and personal security information to the cardholder.

Upon termination of the agreement with the account holder and/or cardholder, or if the bank so requires on objective grounds, the account holder must return, destroy or deactivate the payment card without undue delay. If the account holder wishes to recall the right of disposal, the account holder must notify the bank and destroy the payment card or otherwise prevent it from being used by the cardholder.

6. The payment card's validity period. Renewal

The payment card can be issued for a specific period of validity. Prior to the expiry date, the payment card will be renewed, or the cardholder will receive a new payment card, unless the agreement has been terminated by the account holder or the bank.

The bank will forward updated information about the payment card to Visa, to enable processors and merchants to update their systems, so that fixed and recurring payments associated with the expired card can be maintained based on the new card details. If the account holder does not want such automatic updating, the account holder can contact the bank.

7. Protection of the payment card and personal security information and reporting lost cards

The payment card is personal and must not be transferred or otherwise given to or used by anyone other than the person to whom it was issued. The cardholder must ensure that no unauthorised persons gain access to the payment card. If the payment card is linked to a mobile device (including smartwatches, etc.), the cardholder must exercise due care when storing the mobile device or allowing others to use it.

The account holder and/or cardholder must use the payment card in accordance with the terms and conditions for issue and use. The account holder and/or cardholder must comply with the applicable rules and instructions for use, storage and protection of personal codes/security information (e.g. BankID), and procedures for reporting loss and unlawful acquisition/use, etc.

The cardholder must take all reasonable precautions to protect personal codes and/or other personal security information linked to the payment card.

The personal codes/security information must not be disclosed or made available to anyone else, including the police and the bank. In addition, the codes/security information must not be used in such a way that they can be seen or memorised by anyone else. Personal codes/security information should be learned by heart. If the code/security information nevertheless has to be written down, this must be done in such a way that it is impossible for anyone but the cardholder to recognise it for what it is. Such notes must not be kept near the payment card or mobile devices, including mobile phones, other digital devices or other equipment linked to the payment card.

The account holder or cardholder must notify the bank or the bank's designated assistant without undue delay if the account holder/cardholder suspects or is made aware of loss, theft or unauthorised use or unlawful acquisition of the personal code/security information, payment card or mobile phone, or other digital device or equipment to which the payment card is linked, or unauthorised person gaining knowledge of the personal code/security information, or unauthorised use of the card. The account holder/cardholder must use the reporting options made available by the bank, and otherwise help to ensure that the payment card is blocked as quickly as possible.

Once the notification has been received, the bank will prevent further use of the payment card. The bank will provide the cardholder and/or account holder with confirmation of having received notification and specify the time it was received. It must also ensure that the account holder is able to document having made such notification for 18 months after it was made. The bank will not require payment for such notification.

The account holder/cardholder must notify the bank without undue delay if the payment card or mobile phone, other digital device or other equipment to which the payment instrument is linked, has been found.

8. Using the payment card

When the payment card is used, the account that the payment card is linked to will be debited.

The cardholder must normally confirm the payment with personal security information. The payment card can be used without a personal code/security information or signature, for example for contactless payments or in some cases for online shopping.

If required by the system, the cardholder must instead sign a receipt, debit note or similar debit authorisation. If a signature is used, the cardholder must present satisfactory proof of identity upon request.

When using the payment card, the cardholder may have access to account information as far as the system allows it.

9. Debit limits, etc.

Payment cards can be used within the specified withdrawal and debit limits, e.g. for single transactions, time intervals and total amounts. Debit limits may depend on whether the payment card is used with a personal code and/or other assigned personal security information.

The bank must notify the account holder in the event of significant changes to areas of use and debit limits. If necessary for security reasons, the bank may without prior notice limit the payment card's area of use, reduce debit limits and make other changes to security information or similar. The bank must notify the account holder of such changes without undue delay.

10. Debits

When the payment card is used, the account holder's account will normally be charged immediately. The bank may not debit the account more than 6 months after the payment card is used, unless the cardholder or account holder has consented to this. The bank may nevertheless recover the transaction amount in accordance with the general rules on collection of monetary claims.

11. Reservation

If the merchant (seller/service provider) has a particular need to secure the completion of a subsequent payment settlement, an amount can be reserved in the account. Such reservations require the cardholder's consent. This can be done without obtaining the cardholder's personal code/security information or signature.

Typical situations where reservations may take place are when buying fuel, for overnight accommodation or in connection with the ordering of goods or services by mail order or phone or other forms of distance selling. The reservation will be deleted when the account is debited for the purchase amount. If the cardholder has not accepted a reservation, the cardholder can contact the bank to have the reservation revoked.

12. Retroactive debit

The bank may debit the account holder's account retroactively for certain claims arising in connection with hotel accommodation, car rental or similar, if the cardholder at the time of booking the service or in the agreement with the merchant has accepted such account debit or been made aware of the bank's debit right. Such retroactive debit is done based on the agreement for the hotel accommodation, car rental or similar, and occurs without the cardholder having to once more provide a personal code/security information or signature. Merchants in Norway must provide/send advance notice to the account holder/cardholder of retroactive debits that do not occur in immediate connection with the use of the payment card or card number.

If the amount has been debited the account and the account holder/cardholder disputes liability for the debit, the account holder may make a refund claim in accordance with the rules of section 17 Claims and refunds below.

13. Payment order cancellation

Payment has occurred when a payment order has been approved by the cardholder and accepted by the payment system. The account holder/cardholder cannot suspend or cancel the transaction after this time, unless the debit is made by reservation or retroactive debit and the cancellation can occur under the rules applicable to this.

14. Receipt and own control

The receipt the cardholder gets when using the payment card should be kept for later control against the transaction overview in digital banking services (the online bank, etc.) or other information about account

movements. The account holder or cardholder must notify the bank without undue delay if the information from the bank does not match the cardholder's own records.

15. Overdrafts

The account holder/cardholder is not entitled to debit the account with an amount exceeding the available balance at the time of the debit. The account holder must compensate for unauthorised debits immediately.

In the event of unauthorised overdrafts, the bank has the right to charge the account with an overdraft interest and a reminder fee, if applicable.

Overdrawing the account is considered a breach of contract which, depending on the circumstances and in addition to financial liability, may entail termination of the agreement and criminal liability.

However, if the account holder/cardholder has received inaccurate information regarding the available amount in the account and has debited the account with an amount exceeding the available balance in good faith, the bank cannot charge overdraft interest or other fees until the account holder has been given reasonable time to rectify the matter.

16. Liability in the event of unauthorised use

The account holder is responsible for payment transactions approved in the manner agreed between the account holder and the bank before or after the payment transaction was completed. This also applies if consent to the payment transaction was given via the payee.

The account holder is responsible for all use of the payment card until the bank receives a notification of loss of payment card and/or personal code/security information, cf. section 7 Protection of payment card and personal security information and reporting lost cards. The bank may also hold the cardholder responsible for the use of the card.

After this time, the account holder and cardholder have joint liability for losses if:

- a) the cardholder intentionally or by gross negligence has enabled unauthorised use by others, or
- b) the cardholder and/or account holder failed to notify the bank without undue delay after becoming aware, or after they should have become aware, of loss of the payment instrument or that unauthorised persons have gained knowledge of the personal code/security information, or
- c) the cardholder misuses the payment card or has engaged in or contributed to fraud against the bank.

In any case, the bank is not liable for losses caused by a lack of security, internal control or misuse by the account holder or cardholder.

The account holder's liability under the previous paragraph is not limited to the available amount in the account when the debit was made.

For amounts charged to the account after the bank has been notified that the cardholder is no longer in possession of the payment card, the cardholder and/or account holder is, beyond the circumstances described above, only liable if the bank establishes that it was unable to, or should not have been able to, prevent the withdrawal/payment transaction.

Notwithstanding the above rules, the bank may hold the account holder liable for losses caused by the account holder or cardholder conducting or contributing to fraud against the bank.

Sections 3-7, 4-27, 4-30 and 4-31 of the Norwegian Financial Contracts Act do not apply.

17. Claims and refunds

If the account holder substantiates that a debit has not been authorised and makes a claim under the above liability rules, the bank must reimburse the amount and the interest loss from the time of the debit, provided that the account holder or cardholder makes the claim for a refund without undue delay after the account holder/cardholder was made, or should have been made, aware of the matter, and no later than two months after the time of the debit. The bank must decide its position with regard to the claim within a reasonable period of time. The refund obligation does not apply if the cardholder or account holder has acknowledged liability in writing for the registration of the transaction amount, or the bank has reasonable grounds to suspect fraud. Sections 4-32 and 3-7 of the Financial Contracts Act do not apply.

The refund obligation under the first paragraph furthermore does not apply to any incorrect registrations at the merchant's that the card holder should have noticed when using the payment card to pay for the item or service.

Such claims must be addressed to the seller (merchant). The bank assumes no responsibility for the quality, nature or delivery of purchased goods or services.

If the account holder or cardholder suspects that the cardholder has fallen victim to a criminal offence in connection with the debit, the bank may demand that the account holder/cardholder report the matter to the police.

The account holder or cardholder must provide a written statement to the bank about the circumstances surrounding any loss situation.

If it becomes clear after a reversal that the account holder is still responsible for the debit, the bank may correct the situation by charging the account again.

18. The bank's blocking of the payment card for security reasons, etc.

Regardless of whether the bank has received notification from the account holder/cardholder in accordance with section 7 Protection of the payment card and personal security data information and reporting lost cards, the bank may block the payment card if there are objective reasons related to the security of the payment card or suspicion of unauthorised or fraudulent use. The bank must notify the account holder of the blocking and the reason for this. Such notice is to be given prior to blocking the payment card or, if this is not possible, immediately after blocking the card. If a notice will be detrimental to objectively grounded security considerations or will violate laws or provisions laid down pursuant to laws, the bank may waive providing such notice. Blockings may also be done in the event of the account holder going bankrupt, or in cases of termination or liquidation, cf. the general terms of the account agreement.

19. Technical failure, posting errors or similar

The bank is responsible for the account holder's losses if the account holder's account has been unduly debited as a result of technical failure, posting errors or similar circumstances, including such errors occurring at the merchant's. If the account holder invokes technical failure of the payment system, the bank must substantiate that the system worked as it should have in the time period in question.

The bank is without liability if the payment card cannot be used due to downtime in the payment system, the ATM being out of banknotes or similar, unless the bank has acted negligently. However, such liability in negligence is limited to the account holder's direct losses.

20. The bank's processing of personal data

The bank will process personal data in order to fulfil the agreement with the account holder and to comply with statutory duties, including personal data on natural persons who are role holders, employees, cardholders and users authorised by the company. This will include identification and contact information, and information related to the company's transactions, income, expenses, assets and liabilities. The bank will also process personal data to fight financial crime, money laundering and terrorist financing. For further information about the bank's processing of personal data and contact information for the data protection officer or another responsible person, see the bank's privacy protection statement at www.dnb.no under Protection of personal privacy. Where applicable, the account holder is obliged to inform persons associated with the company about the bank's processing of personal data.

21. Termination

This agreement can be terminated by either party with 1 - one - month's written notice, after which any outstanding balance, including interest and charges, must be paid within the expiry of the notice period. In cases of breach of contract, the bank may terminate the agreement with immediate effect, after which any outstanding balance, including interest and charges, are due immediately. This also applies to card transactions with the addition of transaction price and commissions received by the bank after the card/account contract has been terminated.