Terms of agreement for digital banking – consumer

Version 1.0

1. A brief description of the service

Digital banking means electronic communication channels that provide banking services, for example online banking, mobile banking, including applications (apps) on digital devices, or telephone banking. A digital device could be a mobile phone, a computer, a tablet, a smart watch or other digital equipment.

The agreement enables the accountholder to use digital banking when entering into agreements with the bank, operate accounts, receive and obtain information about accounts and other services, receive electronic invoices and more. The customer dialogue specifies the available functions in the individual channels and guides the accountholder about the use of the service.

2. Account agreements and charges

The terms of agreement for digital banking apply in addition to the digital banking user guidelines, hereunder the customer dialogue included in the service, and the bank's General terms for deposits and payment services. In the event of conflict, the Terms of agreement for digital banking take precedence over the General terms for deposits and payment services.

The costs of setting up, having and using digital banking services are stated in the bank's current price list, on bank statements and/or in another appropriate manner.

3. Security and computer system requirements

The accountholder must use updated software, including operating systems, browsers and other software for safe communication with the bank, as well as antivirus software. Moreover, the accountholder must follow the bank's prevailing instructions and security advice at any given time.

4. Code and security procedure

When entering into an agreement, the accountholder receives a personal code and/or other security credentials and possibly other equipment for use with supplementary security procedures when using digital banking. The accountholder must use this in accordance with the terms for their issuance and use. If the digital banking services are connected to a mobile phone, a digital device or other equipment, the accountholder must take great care to ensure that unauthorised persons cannot access the accountholder's digital banking services.

The accountholder must take all reasonable precautions to protect the personal code and/or other security credentials. The personal codes/security credentials must not be revealed or made available to anyone, including the police, the bank, authorised persons, family members or guardians. Moreover, the codes/security credentials must not be used under such conditions that others can see them or become familiar with them. The personal code/security credentials must be memorised. If the codes are noted down, it must be done in such a way that it is impossible for anyone but the accountholder to understand what the note relates to. Any note containing this information must be kept away from devices, including mobile phones, digital devices or other equipment, used for digital banking.

The accountholder must without undue delay notify the bank or the entity specified by the bank when becoming aware of loss, theft or misuse or misappropriation of the personal code/security credentials or mobile phone, digital device or other equipment used for digital banking, or of unauthorised account access. The accountholder must follow the notification procedures provided by the bank and help to ensure that the security credentials, digital banking services or accounts are deactivated as soon as possible.

Once the notification is received, the bank must immediately prevent any further use of the digital banking services. The bank must confirm to the accountholder that a notification has been provided, including the time it was provided. In addition, the bank must ensure that the accountholder can document such notification for 18 months after it was given. The bank will not claim any compensation for such notification.

The accountholder must immediately notify the bank if the mobile phone, digital device or other equipment used for digital banking is found.

5. Entering into electronic agreements and distribution of electronic information

The accountholder can order banking services and enter into banking services agreements via the digital banking solution. Information about the relevant agreements and how to enter into the agreements is available via the digital banking solution.

The bank will send information about the accountholder's deposits and payment services, for example account transactions and notifications about changes to interest rate levels and costs etc., to the accountholder's digital banking solution.

6. Operation of own accounts

Unless otherwise agreed, the digital banking solution can be used to operate all accounts for which the bank has registered the customer as accountholder. This also applies to accounts opened after this agreement has been entered into.

Accounts operated using digital banking services cannot be debited in excess of the prevailing amount limit. The amount limit is set in the digital banking solution and can be adjusted as instructed by the bank.

The accountholder must not allow anyone else the right or opportunity to operate or gain access to the account or account information using the accountholder's digital banking services.

7. Operation of third party accounts

By agreement with the bank the accountholder can use the digital banking solution to operate a third-party account in the bank. In this case, the third party must authorise the accountholder (authorised person) and enter into an agreement with the bank, allowing their account to be operated in this way.

When the third-party account is operated using the accountholder's digital banking services, the prevailing amount limit established for the authorised person's (accountholder's) digital banking solutions applies, and the authorised person will be able to enter into an AvtaleGiro agreement on behalf of the third party. If the bank offers it, the accountholder can use authorised services to operate the third party's account when this has been arranged for.

8. Authorised services provided by the bank

If the bank offers it, the accountholder, or the authorised person, can via the digital banking solution use payment initiation services and/or account information services (authorised services). On the request of the accountholder, the bank will execute payment initiation services and/or account information services and handle the information necessary to execute the service(s). In this context "the bank" is defined as the bank's role as a provider of authorised services. In this context "account provider" is defined as another bank where the accountholder has a payment account.

In general the accountholder must use the login method and authentication solution that the account provider has supplied to the accountholder. The bank must communicate securely with the account provider and ensure that the personalised security credential of the accountholder is not available to anyone except the issuer of the personalised security credential and the

accountholder, within the bank's competence as a legal representative.

Account information services means that the accountholder, via the bank as account information service provider, will have access to information from one or several defined payment accounts in other banks (account providers). The accountholder consents to the bank contacting the account provider on behalf of the accountholder to request necessary information. The bank is not liable for the account information collected from the account provider being correct and up to date. The accountholder can at any time choose to cancel the account information collection and at the same time withdraw the consent to account information collection from another provider.

Payment initiation services means that the accountholder via the bank in its role as payment initiation service provider can initiate payments from the account provider payment account. The bank is deemed to have received a payment initiation when it has received all the information necessary to execute the initiation. Moreover, the general terms in item 14 apply to the extent that they are relevant. When the bank has received an order, it will communicate the payment order to the account provider, which will initiate the payment transaction. If the initiation is successful, the accountholder will receive a notification from the bank confirming the correct initiation of the payment at the account provider together with an order reference, the amount of the payment transaction and, when relevant, the amount of any fees.

For payment authorisation services the bank is only responsible to the accountholder for the payment authorisation service, not the execution of the payment transaction. The account provider will initiate and execute the payment and is responsible for it. Hence the confirmation of the initiation as mentioned above is only a confirmation of successful initiation not of an executed payment.

An accountholder's claim to refund of a payment as a result of an incorrectly executed or unauthorised payment must be directed to the account provider. The account provider must immediately refund the amount of the missing or insufficient payment transaction to the accountholder and, where applicable, restore the debited account to the state it would have been had the payment transaction not taken place. As the payment initiation service provider, the bank must prove that the transaction is authenticated, correctly registered and not affected by technical failure or some other error.

If the accountholder, via the bank, has initiated a payment transaction from a payment account with another account provider, the accountholder cannot cancel the payment order after the transaction consent has been communicated to the bank.

9. Payment execution

The bank is responsible for executing a payment order from the time the electronic dialogue in the digital banking solution has confirmed the receipt of the payment order.

When paying bills/invoices the reference number identifying the bill/invoice for the recipient (KID, invoice number/customer number or similar) should be stated if available. By not stating the KID number the accountholder runs the risk of the payment being rejected.

Subject to reasonable grounds, among other things that the order is not given according to the service guidelines, the bank may reject the payment order. The system customer dialogue will provide the reason for the rejection.

Payment orders to be executed on a specific day, at the end of a certain period or on the day on which the payer has placed funds at the payment service provider's disposal, can be registered by the accountholder in the digital banking solution to be debited on the day specified by the accountholder (agreed debit date). The payment order is deemed to have been received by the bank on the agreed date if this is a business day, and otherwise on the following business day.

If the accountholder does not want the bank to execute a payment order, the accountholder can, up

to and including the agreed payment day, cancel the order using digital banking functions or contacting the bank. If an order is cancelled, the bank is not liable to pay any interest on overdue payments, collection fees etc. that the beneficiary claims as a result of the cancellation.

The bank will transfer the amount stated on the payment order to the beneficiary's bank at the latest by the end of the business day after the payment order is considered to be received.

Further details about payment executions, including transfer time and the bank's liability in case of delays, can be found in the General terms for deposits and payment services.

10. Electronic invoices

10.1 eFaktura (e-invoice) agreement

The accountholder can enter into an agreement with the bank on receiving e-invoices via the digital banking solution. The e-invoice will then replace the regular paper invoice.

The accountholder accepts the receipt of e-invoices in the digital banking solution. When the e-invoice agreement has been accepted, a unique e-invoice address is assigned to the accountholder. If the bank offers it, the accountholder can choose to use an "alias" instead of the unique e-invoice address. The accountholder can supply the unique e-invoice address (or alias) to invoice issuers providing e-invoices.

In the digital banking solution the accountholder has the right to refuse e-invoices from specified invoice issuers.

If the accountholder has a digital banking agreement or similar access with several Norwegian banks, the e-invoice agreement applies to all banks offering the e-invoice service. The accountholder can, at any time, notify the bank that the accountholder no longer wishes to use the e-invoice service. Such notification will also apply to the digital banking solutions of other banks that the accountholder uses.

If the accountholder has a digital banking agreement with several Norwegian banks, the accountholder can access his or her e-invoices with all the banks offering e-invoice, provided that the accountholder's national identification number is registered with the bank. When the accountholder has paid an e-invoice in one of his or her banks, the information about the paid e-invoice will be available with that bank. If available, the accountholder can also request that e-invoices processed by other banks, and the banks that processed them, be made available. Should the accountholder terminate the digital banking agreement without simultaneously terminating the e-invoice service, e-invoices will still be sent to the accountholder's digital banking solutions in the other banks.

In order to distribute e-invoices to the accountholder's digital banking solutions, the accountholder's name, national identification number, e-invoice address and necessary account information will be stored in a connection registry. The information in the connection registry can be distributed to banks or entities specified by the bank which require the information to be able to distribute e-invoices from the e-invoice issuer to the digital banking solution(s) of the accountholder. The bank of the invoice issuer can also provide the invoice issuer with information about the accountholder's name and necessary contact information. The accountholder's national identification number will only be distributed to invoice issuers with processing purposes in compliance with the Personal Data Act in order to use the national identification number to identify customers in connection with issuing invoices and paying monetary claims. If the accountholder has digital banking services in several banks, the accountholder can choose which bank to contact in case of any alleged errors during the processing of customer details in the connection registry.

The bank is not liable for the contents of the e-invoice and the monetary claim. Nor does the bank

have any influence over which person the e-invoice issuer considers to be the addressee of the claim.

10.2 Invoices received in secure digital mailbox provided by third party

The accountholder can transfer specific invoices/payment claims from their secure digital mailbox for presentation and processing as an electronic invoice in the digital banking solution if the accountholder used a secure digital mailbox and has entered into an agreement with the bank concerning this service. The accountholder can do this even if the accountholder does not have e-invoice agreement with the bank.

11. Erroneous execution of payment orders by the accountholder

A payment transaction, which is credited to the account number stated by the accountholder in the payment order, is deemed to have been correctly executed by the bank, or initiated by payment initiation services, as regards the correct beneficiary. This also applies if the customer has provided further information in addition to the account number. The accountholder must comply with the bank's instructions concerning caution and own check and comply with the bank's notifications about security breaches, errors or other matters.

The bank is not liable for errors made by the accountholder in the payment order, for example incorrect account number for the beneficiary, incorrect KID number, typing errors etc. The same applies to losses due to the wilful or grossly negligent erroneous use by the accountholder.

Nordea

BankID agreement

BankID agreement

Version 1.0

1. Contact details to the Bank

Name: ***Nordea Bank Abp NUF***
Address: ***P.O.Box 1166 Sentrum, N-0107 Oslo, Norway***

URL: ***www.nordea.no***

For blocking your BankID or other questions relating to BankID, please call **(+47)** ***23 20 60 01***

When these terms ask you to notify your bank, you can use the telephone number listed here, or in another way as instructed by your bank.

Notices from your bank will be made to you directly by means of electronic communication such as e-mail, SMS, or the mailbox in your digital bank.

2. About the agreement

This agreement contains the terms and conditions for BankID between you and your bank. These terms and conditions explain what BankID is and specify your obligations as a user of BankID. Read the agreement carefully and contact your bank if you have any questions.

BankID is a common solution operated by the banking sector in Norway. A BankID issued by one bank can be used for other banks and websites, as it is based on a common set of rules. **To make sure BankID is a secure solution, it is important that you keep your BankID private, protect your equipment and password for using BankID, and inform the bank if you suspect others may have gained access to your BankID. See section 4 for details.**

A bank may require you to enter into a customer relationship before issuing you with a BankID.

3. Brief description of the service

BankID is an electronic identification and signing solution issued to you by your bank.

You may use your BankID to log in to Norwegian banks, to verify your identity on public and private websites, and to sign agreements digitally on the internet.

BankID may be used with an app, a code device or code card, a fixed password and your Norwegian national identity number. If you have enabled BankID Mobile, the security elements will include communication between the solution or website relying on BankID and your phone, as well as a PIN-code. BankID may also be used as an app on your smartphone, in which you use the phone's passcode or biometrics, in addition to your password where this is required, to confirm a login or signature.

4. Storing, securing and blocking your BankID

4.1. Your obligation to protect your BankID

To protect your BankID against fraud and unauthorised use, you must take all reasonable precautions to protect your password, codes, equipment, mobile phone and other digital devices you have for using BankID. This means, for example, that you:

- Do not disclose your BankID password or one-time codes to anyone, not even to family members, legal guardians, the Bank, BankID or the police. You must take all reasonable precautions to ensure that no one can see your BankID password or one-time password when you enter it.
- Store your BankID code device in a suitable place, ensuring that it is not openly accessible. If you bring your BankID code device with you outside your home, ensure it is not accessible to others.
- Must choose a strong BankID password that you do not use anywhere else. You can find

guidelines on how to create strong passwords at nettvett.no. Change your password if you suspect that others have come to know it.
- Memorise your BankID password. If you still need to write down your password, it must be done in a manner that ensures nobody else can understand what the password is for. The password must not be kept together with the BankID code device or other equipment or devices.
- Use common sense and be cautious when you use your BankID password and one-time code, especially if you receive links by e-mail, text message/SMS or social media which require you to enter your BankID password or codes. Do not enter your BankID password or one-time codes if you are unsure of the website or that the sender of the link is the one it claims to be.

Keep in mind that you must never, orally or in writing, for example by phone, email or SMS, state you BankID passwords or one-time codes. This also applies where someone pretends to be for example your Bank, BankID or the police.

4.2. Notifying the bank off loss or suspicion of loss of BankID

You must immediately notify the bank if you know or suspect that:

- others, including your spouse/partner or family members, know your BankID password
- you have lost your BankID code device
- your BankID code device is stolen
- you lost your mobile phone or other equipment you use with BankID, or this has been stolen, so that the bank can investigate any unauthorised use of your BankID.
- Someone has misused your BankID

You will not be charged for the bank's costs of issuing a new BankID after notification of loss, unless there are special circumstances on your part, such as repeated notifications of loss.

5. The bank's security measures and blocking of BankID

5.1. Blocking BankID due to loss or suspected loss

After receiving a notification of loss from you, the bank must:

- immediately block your BankID, and
- confirm in writing to you that the notification has been received and that the BankID has been blocked.

5.2. Blocking BankID on the bank's initiative

The bank may on its own initiative block your BankID when your bank has reasonable grounds to believe that:

- someone other than you are able to use your BankID;
- you have not complied with this agreement;
- you will not be able to comply with this agreement.
-

In the event that the bank blocks your BankID, the bank shall notify you and provide information on why your BankID has been blocked and on how you can move forward to have the block lifted.

6. Liability

6.1 General liability

If you negligently or intentionally breach the terms and conditions of this agreement, you may be responsible for any loss incurred by your bank or others, including financial institutions and other solutions or websites relying on BankID, caused by your breach of this agreement.

If the bank negligently or intentionally breaches the terms and conditions of this agreement, the bank may be liable for any loss incurred by you, unless you have acted fraudulently.

6.2 Responsibilities under the Financial Contracts Act

When your BankID is used to confirm payments or sign agreements on financial services, the Financial Contracts Act will regulate your and the bank's respective liability. Breaches of the obligations in this agreement may also be invoked by other providers of financial services when determining whether you are liable for a payment that

has not been authorised or for the misuse of an electronic signature, as set out in the Financial Contracts Act.

7. Termination of the agreement

You are free to terminate the BankID agreement without prior notice, by notifying your bank of the termination in the agreed way. The bank will then block your BankID.

The bank may terminate the agreement if you breach this agreement, e.g. if you breach the obligation to take alle reasonable precautions to protect your BankID-password, one-time codes, equipment, mobile phone and other digital devices you have to use BankID, and there is reasonable grounds to believe that breach of the obligation will occur again .

The bank must notify you of the termination four weeks in advance and include the reason for the termination. The bank can terminate the agreement with immediate effect if you have materially breached the terms and conditions or if you acted contrary to the requirement of honesty or good faith towards your bank or towards other solutions or websites relying on BankID. The reason for the termination must be stated.

When terminating the agreement, the bank may block your BankID immediately, as described in section 5.2.

The bank may also terminate the agreement without specific notice if the customer relationship is terminated.

8. Price and price information

The price of BankID is to be shown in the bank's price list or published in another suitable way.

9. Processing personal data

Your bank is the data controller for your personal data and will process your personal data in accordance with the data protection rules and legislation (GDPR). For further information, see here: www.bankid.no/en/private/protection-of-privacy-and-status/

10. Changes to agreement

The bank may, with two weeks' notice, make changes to the agreement when it has legitimate reasons for doing so. This includes price changes, changes caused by altered functionality or changes due to legislation. If the change is to your disadvantage, such as a price increase, the bank will notify you 2 months before the change comes into effect.

If security-related factors so require, the bank may without prior notice limit the area of application of your BankID or make other changes in security procedures or similar. The bank must notify you as soon as possible after such a change has been made.

11. Dispute resolution

If a dispute arises between you and the bank you have entered into an agreement on the use of BankID with, you can bring the case before the Norwegian Financial Services Complaints Board (FinKN) for consideration, provided the case is within the board's authority, and you have an objective interest in obtaining the board's consideration. The bank may bring a dispute about the use of BankID before the FinKN when your BankID has been used to confirm payment transactions.

If BankID is used to authorise a payment transaction that you deny having consented to, there are provisions in the Financial Contracts Act on what you must do, and on your bank's obligations. Further information on that what you should do can also be found in the account agreement between you and your bank.

Enquiries to FinKN are to be sent to Finansklagenemnda, Post box 53, Skøyen, N-0212 Oslo. Telephone no. (+47) 23 13 19 60. For further information, see www.finkn.no.