Terms and conditions for electronic communication – online services

1. Scope of application

These terms and conditions apply to electronic communication undertaken by the Customer or the User using eBanking, mobile banking services or telephone services (hereinafter online services) when the Customer or the User contacts the Bank or when the Bank makes telephone contact with a Customer or User who uses bank identifiers. These terms and conditions were adopted on 1 September 2024.

If the customer is a consumer and uses payment services as defined in the Payment Services Act (290/2010), the Bulletin on payment service is also applied in addition to these terms and conditions.

In the event of discrepancies between the different language versions of the terms and conditions, the Finnish version takes precedence.

2. Identifiers and user rights

2.1 Electronic identification and electronic signature

The online services can be used with identifiers, such as bank identifiers accepted by the Bank. The identifier is the tool used by a natural person to identify him/herself electronically and make electronic signatures.

When the Customer or the User contacts the Bank, the Bank identifies the Customer or the User on the basis of the identifier; at the same time, the Customer or the User identifies the Bank. The use of the identifier corresponds to the Customer's or the User's identification via a traditional identity document (electronic identification).

When the Bank contacts the Customer or the User by telephone, the Customer or the User identifies the Bank from the calling number and by the way the Bank acts, as set out on the Bank's website (see "A phone call from the Bank"). The Bank identifies the Customer or the User on the basis of the information collected before the contact and received during the call. The use of such information corresponds to the Customer's or the User's identification via a traditional identity document.

When the Customer or the User accepts or confirms service requests in the online services using his/her identifier, the use of the identifier is equivalent to the Customer's or the User's personal handwritten signature (electronic signature).

The Customer or the User and the third party shall separately agree on the legal effects of the use of identifiers in connection with the use of the Bank's identification service and web payment service.

2.2 Acting electronically on behalf of the Customer

The natural person may act on behalf of the Customer in the User's role in the online services when user rights have been linked to the User's identifier. The range of user rights varies between different channels, data terminal equipments and roles.

User rights can be based on authorisation, law or order of the authorities. When user rights are assigned, all the documentation on which the user rights are based must be presented to the Bank at its request.

The User shall make transactions on behalf of, in the name of and on the account and at the responsibility of the Customer. The Customer is responsible for all service requests which the User makes in the online services during the period of validity of his/her user rights. The Bank has no responsibility to either the Customer or the User for damages arising due to the fact that the User has used or stored his/her identifiers without due care.

The Bank shall suspend user rights at the Customer's or User's request. The Bank shall change user rights only at the Customer's request. The Customer or the User must notify the Bank immediately if he/she wants to suspend or change user rights. User rights shall cease and the responsibility of the Customer shall end once the request has been made, the Bank has received the request and the Bank has had a reasonable period of time in which to make the change. The Bank does not have a duty to inform the Customer or the User of the suspension or change of user rights.

2.3 Safekeeping of and responsibility for lost identifiers

The identifiers are personal and they must not be handed over, even partly, to a third party or for use by other persons, applications or services. Notwithstanding the foregoing, the

Customer may use, in accordance with his/her own consent, identifiers to perform the services in the systems provided by registered payment service and account information service providers referred to in the Payment Services Act (30.4.2010/290)

The Customer and the User undertake to carefully safeguard the identifiers approved by the Bank according to their instructions so as to prevent them becoming known to or being used by any unauthorised person.

The Customer undertakes to keep the user ID, code calculator, ID app, password, PIN codes or other means of identification approved by the Bank and constituting bank identifers separate from each other. The password must preferably be committed solely to memory and not kept written down. When the Customer or the User receives a new bank identifier, the password assigned by the Bank must be changed immediately.

The Customer is responsible for the safekeeping of identifier data in its possession so that unauthorised persons cannot gain knowledge of it. The Bank will never ask for information relating to bank identifiers via e-mail or otherwise when contacting the Customer or the User. Identifier information should never be given out by e-mail or by telephone to anyone who requests it, not even to the Bank.

The Customer or the User must notify the Bank immediately if he/she knows or suspects that a bank identifier, secret password, telephone or other mobile device containing the bank identifier app, code calculator, telephone fitted with rapid identification or information relating to same has come into the knowledge or possession of an unauthorised person.

The use of bank identifiers can be prevented via the blocking service provided by the Bank. The notification must be made immediately and it can be made:

- personally at the bank's branch during its opening hours
- to the Bank's customer service, tel. 0200 2580 (local network charge/mobile network charge). The current opening hours of customer service and branches can be found on our website
- by telephone round the clock to the number of the Bank's 24h Card service receiving loss or blocking notifications, 0200 2585 (local network charge/mobile network charge) or, when calling from abroad, +358 200 2585 (local network charge/mobile network charge)

The Customer's or the User's responsibility for unauthorised use of the identifier shall cease once the Bank receives notice of its loss. The blocking of bank identifiers in eBanking or in telephone services shall also be considered as notice of loss.

If bank identifiers are meant for corporate use, the corporate Customer has the right to terminate the bank identifiers if the company has removed all user rights from them and the bank identifiers do not include authorisations from other companies or institutions, meaning that the identifiers are therefore not required.

The Bulletin on payment service is applied to the obligations and responsibilities related to the use of payment transactions by customers in a consumer position.

2.4 Use of biometric authentication

The use of bank identification or other electronic services may require the authentication of the Customer or User on a mobile device. The technology of the Customer's or User's mobile device may support different authentication methods, such as PIN code or biometric authentication. If the Customer or User wishes to use biometric authentication, he/she must ensure before using the service that only his/her own biometric data, such as fingerprints, face recognition data or any other biometric data, is stored on his/her device.

Biometric data stored on a mobile device can be used for authentication instead of or in addition to a PIN code. Service-specific restrictions on the use of biometric authentication may apply to some services. The Bank is entitled, without notice, to make changes to these service-specific restrictions or to prevent the use of biometric authentication.

If the Customer or the User has selected facial recognition authentication from the biometric authentication options, the mobile device may not be given to a third party to prevent misuse.

Identification in the authentication app using biometric authentication is equal to identifying with other bank identifiers. The Customer or the User agrees to any legal action he or she has approved using by using biometric authentication.

In addition to these terms and conditions, other instructions and advice provided by the Bank on the safe use of bank identifiers shall apply to biometric authentication.

3. Range of services

The financial services of the Bank and products and services produced by third parties are offered via the online services. The range of services available may vary between different channels, data terminal equipments and roles.

The online services contain confidential information about the Customer, the User and the financial services he/she uses,

as well as usage information on those services. The Customer or the User may use financial services and agree on new financial services via the online services to the extent that this is possible.

The financial service-specific terms and conditions shall take precedence for service requests made via the online services. In the second instance, these terms and conditions shall apply. These terms and conditions are available in English, Finnish and Swedish. In the event of any conflict between different language versions, the Finnish version shall take precedence.

4. Intellectual property rights

The ownership, copyright, trademark and all other intellectual property rights relating to the online services and financial services are the property of the Bank unless otherwise stated. The borrowing, copying, recording, editing, variation, transfer, other exploitation or utilisation of the content or part of it without advance written permission from the Bank is expressly forbidden.

5. Customer data and transaction information

5.1 Provision of information

The parties are obliged

- to provide adequate identity information and contact information, such as the official name, identity number or other ID information, address and telephone number
- to communicate new identity information and contact information in the event of any changes.

The parties are responsible for the validity and correctness of the information given.

The Bank's official identity and contact information is published on the Bank's website. The Bank's Identification principles are available at www.danskebank.fi/pankkitunnukset.

The Customer and the User are obliged to inform the Bank immediately in the event of any changes or incidents which are relevant in terms of the Customer's or User's responsibility, such as information

- relating to the loss of the identifier or the traditional document used to authenticate the identity of the Customer or the User
- relating to the beginning or end of trusteeship, or relating to a death.

5.2 Recording and storing of information

The Bank has the right, without informing the Customer or the User

- to save and file log information based on the use of the online services
- to save and file service requests made via the online services
- to record and file conversations with the Customer or the User via telephone services.

The information based on the use of the online services and transactions made in the online services form part of the Bank's Customer Register. The information relating to identification shall be retained for as long as is required by law. Other information shall be retained as long as is necessary from a risk management point of view. After these deadlines, the information will be destroyed.

The Bank has a right to collect information as follows:

- details about the computer used by the Customer or the User, such as information about the operating system and browser version
- information about the usage of the Bank's services during the session.

5.3 Use of information

In addition, the Bank has the right to use the recorded calls for verifying assignments, developing its customer service, risk management purposes and as evidence in the settlement of any disputes.

Concerning other recordings and databases, the Bank has the right to use customer and transaction data for purposes mentioned in the privacy notice valid at the time. The Bank may combine personal and transaction data with website browser and application data and store this information.

Information collected by using security software or otherwise about

- the computer used by the customer or the user will be used in order to protect the customer and the user against security or information security attacks and the attempts to misuse the services, and to develop information security solutions and for business development purposes, to monitor personal online behaviour and to offer targeted marketing and contact the customer
- the usage of the Bank's services during the session will be used for statistic and business development purposes, to monitor personal online behaviour and to offer targeted marketing and contact the customer.

The Bank may only assign customer data to third parties if the Customer or the User, within the limits of the user rights, has given prior consent to the Bank, the Bank is allowed to assign the information on the basis of the law without the Customer's or the User's prior consent or the Bank is obliged to assign the information on the basis of the law or by official order of the authorities.

5.4 Enquiries

The Customer or the User may ask to have information on him/herself recorded in connection with the use of the online services and listen to individual telephone conversations that have been recorded by submitting a request to the Bank. The Bank may supply the information to which the request relates if

- the Customer or the User has been reliably identified
- the Customer or the User has the right to receive the information in accordance with secrecy regulations
- the information relates to the individual event and
- the request is justified.

The information shall be supplied without charge if the request relates to one event and only one request is made per year. Otherwise the Bank shall charge the fees set out in the pricelist.

6. Distribution of responsibility

6.1 Information about the financial services

When the Customer or the User makes a service request, the Bank is responsible for providing all the necessary information, such as information about the product company, key information on the financial services, and the terms and conditions, prices and information relating to distance selling.

If not otherwise agreed, the financial services are chargeable. The Bank shall charge the payments and fees on the basis of the pricelist from the Customer. The charges shall be debited to the Customer's account if the Customer has an account with the Bank.

6.2 Devices, programmes, systems, extensions and their use

The Bank has set out on its website the minimum technical specifications for using the online services. The Customer or the User is responsible for ensuring they have adequate devices, programmes and systems in place, such as data terminal equipment, browsers, subscriptions and telecommunications. The Bank provides no guarantee that the online services can be used with the Customer's or the User's hardware, software, systems and connections.

The parties shall be responsible for the procurement, use and maintenance of their hardware, software, systems and the necessary data communication connections, including their costs and expenses. The parties shall be responsible for ensuring that the hardware, software, systems or connections or the use thereof to access the online services does not give rise to damage, interference or other injurious effects to the parties or to third parties.

6.3 Safety and information security

The Bank's website includes information regarding safety issues. Information about the hardware and software requirements based on prevailing information security threats is also available on the website of the Finnish Communications Regulatory Authority.

The Customer and the User are responsible for ensuring that they have

- adequate devices, programmes, systems, extensions and especially information security software as required from an information security perspective
- adequate software and information security update processes.

The Customer and the User are responsible for costs and expenses arising in connection with the above measures.

In order to ensure the safe use of the online services, the Bank recommends that the Customer and the User should

- regularly read information provided by the Bank and the Finnish Communications Regulatory Authority regarding information security information and guidelines
- make his/her best reasonable efforts to ensure that the equipment, hardware, software, systems and the necessary data communication connections are sufficiently secure and that both these and the data security systems are updated regularly.

The Bank will inform either the Customer or the User of any threats regarding fraudulent activities or security using the contact details provided by the Customer or the User, or announce them generally in the Bank's electronic channels.

6.4 Service requests

6.4.1 Online services

The Customer or the User may make service requests via the online services. The service request shall be final and binding once the service request reaches the Bank's systems and the online service notifies the Customer or the User that the request has been received, unless otherwise agreed.

The Customer shall be responsible for all transactions and service requests made using the Customer's identifier. The Customer shall also be responsible for transactions and service requests which have been made by the User nominated by the Customer.

6.4.2 Secure messaging

The Bank has the right to send confidential information to the Customer or to the User in electric form using secure messaging, which is part of eBanking.

6.4.3 Online meeting

An online meeting is a meeting between the Customer and the Bank in the online conference area provided by the Bank. The Customer and the Bank will communicate during such a meeting using image and audio.

An invitation to an online meeting is always sent using the Bank's message system. The Bank reserves the right to use systems provided by third parties when implementing the online meeting service. The Bank has the right to show and reveal to the Customer or the User confidential information during an online meeting, provided that the Customer or the User has agreed to sharing such information.

The discussions conducted by the Customer and the Bank in an online meeting may be recorded.

6.4.4 Electronic mailbox

The Bank has the right to send different personal messages and documents in electronic form for the customer or user to the electronic mailbox, when the customer has taken the electronic mailbox into use or has authorised a user to receive customer's messages and documents to the electronic mailbox.

Additional information on the electronic mailbox and the list of messages and documents sent to the electronic mailbox is available on the Bank's website at www.danskebank.fi. The bank has the right to change the abovementioned list in the way agreed in section 7.1 in this agreement.

Despite the use of the electronic mailbox

- the customer or user, if he/she so desires, can order a paper version of a message or document sent to the electronic mailbox, in which case the Bank will charge a fee for the delivery according to the service price list
- the Bank, if it so desires, always has the right to send messages and documents to the customer or user in paper format by mail.

6.4.5 Message services

The Bank has the right to send the Customer or the User a text message reminder of an unconfirmed service request made in telephone services without the Customer's or the User's consent.

In addition, the Bank has the right to send the Customer or User confidential information as a text message or via ordinary e-mail if this has been agreed in advance.

If the Customer has adopted the Bank's message service, an agreement concerning the message service arises between the Bank and the Customer. The provisions of these terms and conditions concerning message services and the Bank's guidelines concerning the service are applied to the service.

The Bank sends the Customer agreed information to the mobile telephone number, e-mail address or other electronic address designated by the Customer. The Bank delivers the information to the mobile telephone number, e-mail address or other electronic address designated by the Customer.

The Bank has confidence in the correctness and up-to-date nature of the information provided by the Customer.

The Customer is responsible for the validity of the mobile telephone number, e-mail address or other electronic address provided by him/her and the correctness and up-to-date nature of the information provided. The Customer is obligated to immediately inform the Bank if any changes take place in this information.

Information sent via the message services is confidential and subject to banking secrecy. When the Customer has adopted the service, the Bank has the right to send such information.

The use of ordinary e-mail does not guarantee that the information sent remains unchanged and confidential. E-mail is used in message services at the Customer's own risk.

The Customer may stop using the message service by informing the Bank of this in eBanking or at a branch office.

When the Customer stops using his/her mobile telephone or changes his/her mobile telephone number or e-mail address that is attached to the message service pursuant to this agreement, the Customer shall inform the Bank of the new mobile telephone number or e-mail address. In other cases, Customer-specific information subject to banking secrecy may become known to the new holder of the number or e-mail address.

Service fees in accordance with the service price list are charged for the use of message services.

6.4.6 Customer's accounts with other banks – account information and payment order service

If the Customer has activated the bank's Account Information Service, an agreement for the Account Information Service is established between the Bank and the Customer.

The Account Information Service is an online service that provides compiled information about one or more payment accounts held by the Customer, which are usually managed by one or more payment account providers (hereinafter "Account Information Service"). The Account Information Service

is available through the channels provided by the Bank at any given time.

The Customer shall use the identifiers provided by the payment account provider to access the Account Information Service and account information. The Customer gives the Bank separate consent to collect account information for each payer account provider. The Customer can determine from which accounts of the selected payment account providers the information is collected.

The Bank does not process the Customer's account information provided by payment account providers, and the Bank does not have access to this information except when providing the Customer with an Account Information Service in accordance with Section 82b of the Payment Services Act (30.4.2010/290).

The Account Information Service uses the Customer's account number, balance, account transactions and account name. The Bank can combine personal information and account transaction information.

The Bank can not guarantee the accuracy of the information in the Account Information Service. The Bank is not responsible if the Account Information Service is not available or any of its features does not work. The Bank shall not be responsible for financial decisions or other decisions made on the basis of the Account Information Service.

The Customer and the Bank have the right to terminate the Account Information Service separately as described in the section "Validity and termination of the agreement" of these Terms and Conditions.

If the Customer has terminated the Account Information Service, all data that has been collected will be deleted with the exception of possible statutory data.

The Customer can also use Danske Bank's Online Services to make payment orders from his or her accounts with other banks. The Customer accepts the transfer using the account bank's own online banking solution and the transfer is executed in the Customer's account bank.

Once accepted, an account transfer cannot be cancelled.

The bank transfer can be verified by updating the details of the relevant account in Danske Bank's Online Service app. Execution of a payment order can also be checked with the help of the other bank's online service solution.

Danske Bank is not responsible for decisions and transactions made by the Customer on the basis of the information in the Account Information Service. Danske Bank is not responsible for the temporary unavailability of the service or for the fact that all features of the function are not in use.

6.5 Restrictions or interruptions to the service

6.5.1 Planned break of service

The Bank has the right to interrupt online services or an individual financial service if the break is planned and information about the break has been provided beforehand both via the online services and on the Bank's website.

6.5.2 Safety and information security threats

The Bank has the right to block the use of identifiers for security reasons if the identifiers have not been used within a reasonable period of time or the identifiers have not been used for a long time.

The Bank has the right to restrict the use of the online services or interrupt it in order to protect customers and users from threats to safety or information security.

The Bank can

- change the requirements as regards devices, programmes and tools needed to use the online services
- change the protection level of the logon or close the identifiers
- slow down assignments and other service requests given in the online services
- block the use of individual financial services or the use of the online services
- block the use of identifiers if they are used as a payment instrument and the bank has grounds to cancel the payment instrument in accordance with section 57 of the valid Payment Services Act (30 April 2010/290).

The Bank has the right to block the Customer or the User from using individual financial services or the online services in the event that the devices, programmes, systems or extensions used by the Customer or by the User cause damage, disturbance or otherwise endanger the safety or the actions of the Bank, other Customers or Users.

6.6 Own behaviour

The Bank has the right to prevent the use of the Customer's or the User's identifier if

- the Customer or the User does not comply with the terms and conditions of the online services or financial services or the related instructions or
- The Bank has reasonable grounds to suspect that the identifiers, the online services or financial services are

used illegally, immorally or in a way which may cause damage to the Customer, the Bank, third parties or outsiders.

If the Customer or the User deliberately tries to prevent or disturb the use or usability of the online services, connecting to the service continually without justifiable reason and thus causing damage or disturbance to the Bank, its Customers, third parties and/or outsiders, the Bank has the right to block the use of the Customer's or the User's identifiers, end the customer agreement and demand full compensation for all direct and indirect damages that have been incurred.

6.7 Execution and interruption of service requests

The Bank is responsible for carrying out service requests in the agreed time if the service request has been submitted with the identifiers. The Bank does not have a duty to carry out service requests if the Customer or the User has not been reliably identified.

The Bank is responsible for ensuring that the content of service requests received by the Bank does not alter whilst in the Bank's control. However, the Bank is not responsible for damages caused by the disappearance of or changes to service requests in areas outside the Bank's control such as the public data network.

The Bank shall carry out service requests on the basis of the information provided by the Customer or the User. The Customer and the User are responsible for ensuring the validity and correctness of the information provided in the service request. If the service request or the related information are incorrect or defective or the service request is otherwise unsuitable for execution for reasons attributable to someone other than the Bank, the Bank shall not be obliged to fulfil or execute the service request and may interrupt or refuse the service request.

The Bank has the right not to execute the service request if

- the Customer or the User does not comply with the terms and conditions of the online services or financial service or the related instructions or
- the Bank has reasonable grounds to suspect that the online services or financial services are used illegally, immorally or in a way which may cause damage to the Customer, the Bank, third parties or outsiders.

The Bank has no obligation to inform the Customer or the User if the service request is not fulfilled or executed due to one of the reasons mentioned above.

6.8 Defect and liability for damages

6.8.1 Complaint

Complaints and claims relating to the online services or financial services must be submitted to the Bank without delay, at the latest within one (1) month of the date the Customer or the User noticed or should have noticed the grounds for the complaint or claim. Complaints or claims regarding financial services must be submitted directly to the product company.

6.8.2 Availability of online services

The Bank shall inform customers and users of technical problems and service breaks in online services on the Bank's website and/or on the login page of eBanking or mobile banking services. During service breaks in eBanking or mobile banking services, alternative service channels such as telephone services, automated teller machines and branch offices can be used during office hours.

The use of eBanking requires that the customer's or user's computer meets certain requirements for instance the browser type, JavaScript and java capabilities as specified in 6.2. The Bank shall not be responsible for any technical problems or damages arising because the Customer's or User's computer does not meet these technical requirements or if these requirements cause him/her technical problems.

Regarding breaks of the eBanking service the Bank is responsible for direct damage when

- eBanking or mobile banking services are not available for reasons caused by the Bank
- a break of service is not planned and was not communicated by the Bank beforehand via the online services
- the Customer or the User does not have alternative service channels reasonably available and as a result of a break of service the Customer or the User must pay additional travel costs and service fees because he/she must use an alternative service channel for matters which cannot be carried out at a later date.

The Bank is not responsible for any other damages resulting from breaks of service.

The Bank has the right to block

- the use of identifiers by all customers, the use of individual data terminal equipment or the use of an individual financial service if the interpretation of a law or order of authorities referred to above has changed
- the use of a single identifier or a single financial service if the individual Customer or User has moved out of Finland or the Customer's or User's domicile is elsewhere than in Finland

and if the Bank's opinion is that the change might give rise to unpredictable legal risks or claims against the Bank.

The Bank shall block the use of an identifier if the Customer or the User of the identifier dies and the Bank receives notification of the death. The Bank shall remove the user rights connected with the identifier if the Customer who was assigned the user rights in question dies and the Bank receives notification of the death.

6.8.3 Indirect damage

The Bank shall not be responsible for any indirect damage such as that arising from the loss of an arrival or income, from interest loss, from a yield that was not received, from diminishing returns or business interruptions, from agreements between a Customer and User or a third party or from the failure of such to come true or from other claims submitted to the Customer by third parties.

6.8.4 A Consumer Customer's responsibility for the use of bank identifiers as a means of payment in Danske Bank's Online Service

If online bank identifiers have been used without authorisation as a means of payment in the Online Service, the Consumer Customer is liable for any damages resulting from the unauthorised use of bank identifiers and for commitments and orders made using the online bank identifiers if:

1) the Consumer Customer has handed over the identifiers to a third party or handed over the service connection opened with the identifiers for the use by a third party;
2) the loss, unauthorised possession or use of identifiers is due to the negligence of the Consumer Customer or the Consumer Customer's neglect of his or her obligations under these terms and conditions; or
3) the Consumer Customer has failed to notify the Bank or blocking service of the loss, unauthorised knowledge or possession by another person or the unauthorised use of the identifiers without undue delay after discovering it.

In the case referred to in section 1 above, the Consumer Customer is liable in full for any damages resulting from the unauthorised use of the identifiers and in the cases referred to in sections 2 and 3 up to a maximum of EUR 50. Nevertheless, the Consumer Customer is always fully liable for damages if they have acted intentionally or through gross negligence.
The Bank is responsible for the unauthorised use of the Consumer Customer's identifiers in the Online Service, despite the fulfilment of the Consumer Customer's liability criterion referred to in sections 1, 2 or 3 above, as follows:

1) the Bank is liable for damages to the extent that the identifiers have been used after the Bank or the blocking service has been notified of the loss, unauthorised knowledge or possession or the unauthorised use of the identifiers by a third party.
2) the Bank is liable for damages if the Bank has not ensured that the Consumer Customer has an opportunity to report at any time the loss, unauthorised knowledge or possession of the identifiers or their unauthorised use by a third party. However, notwithstanding the above, the Consumer Customer is fully responsible for the unauthorised use of identifiers in the Online Service if they have intentionally made a false report or otherwise acted fraudulently.

6.8.5 Consumer Customer's responsibility for the use of bank identifiers as strong e-identification

If the identifiers have been used without authorisation as strong e-identification, the Consumer Customer is liable for the damages resulting from the unauthorised use of the identifiers and for the commitments made with them if:

1) the Consumer Customer has handed over the identifiers to a third party or handed over the service connection opened with the identifiers for the use by a third party;
2) loss, unauthorised knowledge or possession by another person or the unauthorised use of the identifiers is due to other than the minor negligence of the Consumer Customer; or
3) the Consumer Customer has failed to notify the Bank or blocking service of the loss, unauthorised knowledge or possession by another person or the unauthorised use of the identifiers without undue delay after discovering it.

In the cases referred to above, the Consumer Customer is liable in full for any damages resulting from the unauthorised use of the identifiers.

Nevertheless, the Consumer Customer is not liable for the use of identifiers without authorisation as strong e-identification despite the fulfilment of the liability criterion referred to in sections 1, 2 or 3 above:

1) to the extent that the identifiers have been used after the Bank or the blocking service has been notified of the loss, unauthorised knowledge or possession or the unauthorised use of the identifiers by a third party;
2) if the Bank has not ensured that the Consumer Customer has an opportunity to report at any time the loss, unauthorised knowledge or possession of the identifiers or their unauthorised use by a third party; or
3) if the service provider using the identification service provided by the Bank has not checked the systems or registers maintained by the Bank for the existence of a restriction of use of the identifiers or information on the blocking or closing of the use of identifiers.

6.8.6 Special terms and conditions concerning the liability of business and corporate customers

Business and corporate customers are liable in full for all actions and damages based on the use of online bank identifiers

until the Bank has received a notification of the loss, unauthorised knowledge or possession of the identifiers or their unauthorised use by a third party and the Bank has had reasonable time to prevent the use of the service. However, business and corporate customers are also liable for all damages to the extent that the identifiers have been used after the Bank or blocking service has been notified of the loss or unauthorised knowledge or possession of the identifiers or their unauthorised use by a third party, if the business or corporate customer has intentionally made a false report or otherwise acted fraudulently.

Business and corporate customers accept vis-à-vis the Bank that a User acting on behalf of the business or corporate customer always has access to the accounts connected to the Online Service of the business or corporate and other services included in the Online Service, even if the Bank has not been separately notified of this.

6.8.7 Force majeure

The parties shall not be responsible for damage resulting from a force majeure event which the party cannot influence and which makes the parties' actions excessively more difficult. The parties have a right to interrupt for the duration of the force majeure event the tasks and duties set out in these terms and conditions. Examples of a force majeure event include

- war, threat of war, revolt or riot;
- industrial action such as a strike, block, boycott or blockade even if this does not affect the party at all;
- disturbances outside the parties' control, such as to automatic data transfer, the public data network or the electricity supply;
- catastrophe, epidemic, disaster or other serious external threat which is comparable to the events mentioned above and independent of the parties.

Each party is obligated to inform the other party of a force majeure event as soon as possible. If the force majeure event concerns the Bank, the Bank may announce the force majeure on its website or in national daily newspapers.

6.8.8 Agreement between the Customer and third parties

These terms and conditions shall not apply to products and services provided by third parties. The Bank

- shall not be responsible for the information given by third parties in respect of its products, services and the safety of same
- shall not be a party to any such agreement or transaction
- shall not be responsible for any duties, mistakes or delays on the part of third parties
- shall not guarantee the solvency of third parties or the features of their products and services.

7. Changes

7.1 Range of services

The Bank has the right to change the online services, the range of financial services and the features of an individual financial service

- without informing the Customer or the User of it beforehand
- by taking into account the new financial service, fees, instructions, functionality, appearance, user interface, content, usability, availability and demand of devices and programmes required for use and
- by communicating the change, if necessary, on the Bank's website.

7.2 Terms and conditions

If there is any need to change the terms and conditions of this agreement, the Bank shall inform customers and users of the change by publishing the amended terms and conditions on the Bank's website if the change:

- is the result of a change in the law or an order or decision on the part of the authorities;
- does not concern matters governed by the Payment Services Act (290/2010); or
- has been made on the initiative of the Bank but does not significantly increase the duties of the Customer or the User or significantly reduce their rights.

In such cases the change shall become valid once it has been published on the Bank's website.

However, if the change

- is the result of a change in the law or an order or decision on the part of the authorities or
- has been made on the initiative of the Bank and does significantly increase the duties of the Customer or the User or significantly reduces their rights,

the Bank must notify the Customer and the User of the change in the terms and conditions of this agreement in advance, via the online services or by post. The change shall become valid at the earliest two (2) months after the above notification is sent. If the Customer or the User disputes the change, he/she can terminate this agreement.

The Customer and the User are considered to have accepted the change

- if they have received notification of the change and continue to use the online services or
- two (2) months have elapsed from the sending of the notice and the Customer or the User has not notified the Bank within this time that he/she disputes the change.

8. Validity and termination of the agreement
This agreement is valid until further notice.

The Customer or the User may terminate this agreement immediately by notifying the Bank. The Bank may terminate this agreement by giving notice of termination; the agreement will then be terminated after two (2) months. The notice of termination can be made via the online services, by post or at the Bank's offices.

The Bank shall carry out all service requests made during the validity of this agreement. During the notice period, the Customer shall be responsible for all liabilities and obligations related to this agreement and the service request made in the Customer's name. The Customer's and the User's right to use the online services shall cease when this agreement has been terminated.

The Bank has the right to dissolve this agreement if the use of identifiers, the online services or financial services has been interrupted as a result of malpractice or an essential breach of contract on the part of the Customer or the User. The notice of dissolution can be given via the online services, by post or at the Bank's offices.

9. Target country, applicable legislation and place of jurisdiction
The online services have been designed to meet all domestic legal requirements. Therefore

- the online services are intended only for the Finnish market
- Finnish law shall apply to this agreement, the online services and financial services irrespective of which country the online services are accessed from.

In the event of any dispute between the Bank and the Customer or User with regard to this agreement that cannot be resolved through negotiation, the dispute shall be resolved in the district court under whose jurisdiction the Customer's Bank's registered office falls or its administration is primarily managed or in the district court of a Finnish locality under whose jurisdiction the Customer's domicile or permanent residence falls. If the Customer does not have a residence in Finland, any disputes shall be resolved in the district court under whose jurisdiction the Customer's Bank's registered office falls or its administration is primarily managed.

10. Customer guidance and authorities
If you have any questions concerning these terms and conditions and the online services, please contact the Bank in the first instance by sending a message using eBanking's secure messaging, by using the form on the Bank's website or by calling the Bank on +358 200 2580 or eBanking Customer Support on +358 200 2589.

Furthermore, the Customer or the User can always, if desired, contact

- The Finnish Financial Ombudsman Bureau, Porkkalankatu 1, FI-00180 Helsinki, Finland., tel. +358 (0)9 6850 120 Mo – Fri 9 – 16.
- The Financial Supervisory Authority, Snellmanninkatu 6, P.O. Box 103, 00101 Helsinki, tel. +358 (0)10 83151.
- Finnish Competition and Consumer Authority, Haapaniemenkatu 4 A, 7th floor, P.O Box 5, 00531 Helsinki, tel. +358 (0) 29 505 3000.
- The EU Commission's online complaint portal at ec.europa.eu/odr. If you file a complaint on the complaint portal, you must state Danske Bank's e-mail address, which is danskebank@danskebank.fi.
- The Finnish Communications Regulatory Authority, Itämerenkatu 3 A, P.O. Box 313, 00181 Helsinki, tel. +358 (0)9-69 661.

11. Privacy notice
We register and use data about you to offer you the advice and solutions, and to comply with the legal requirements that apply to us as a financial institution. You can read more about what data we register, how we use it and your rights in our privacy notice www.danskebank.fi/privacystatement, which can also be provided in hard-copy for you. The notice also provides contact information if you have questions.

Definitions
Bank = Danske Bank A/S, Finland Branch and its subsidiaries. These companies have been listed on the Bank's web pages.

Bank identifiers = identifiers provided by the Bank that consist of identification tools and identifying data or features and that, when used together, provide the identifiers required to access the service, as well as the tools for identifying and authenticating. Channel-specific identification tools may be used for the Bank's different channels. The Bank and the Customer shall agree individually the method to be used. The use of bank identifiers corresponds to the Customer's binding signature. Bank identifiers are personal and may not be disclosed for use by other persons.

Bank identifiers may be either strong identification devices in accordance with the Act on Strong Electronic Identification

and Electronic Trust Services (617/2009) or so called weak identification devices.

Biometric authentication = Authentication of identity by the physical characteristics of a person, such as a fingerprint or facial features.

Confidential information = information about the Customer, the User, his/her financial services or the use of same. Such information is subject to bank-client confidentiality and other secrecy regulations.

Content = trade name, characteristic, domain name, source code, appearance, text, picture, voice or other immaterial content.

Control area = information system which is in a party's possession, control or sphere of influence such that said party can influence and take responsibility for it. The Bank's control area refers to the information technology environment inside the outermost firewall of the Bank's information processing systems.

Customer = a private individual (natural person) or corporate body (legal entity) that is a Customer of the Bank by virtue of the agreement concerning the product or service offered by the Bank.

eBanking = a browser- or application-based Internet service provided by the Bank, access to which is controlled by means of an identifier.

eBanking archive = an electronic archive in the Customer's eBanking service for storing the Customer's documentation.

Financial service = individual product or service, such as an account agreement or card transaction information.

Identification service = service via which the Customer or the User can identify him/herself electronically using his/her identifier and can make electronic signatures if these legal effects have been agreed with the third party, such as an authentication app.

Identifier = bank identifiers or another identifier accepted by the Bank which is used by the Customer or User. The Bank identifies the Customer or the User electronically on the basis of the identifier. The Customer or the User can make electronic signatures using the identifiers.

Message system = a tool available in the Customer's eBanking service used for communications between the Customer and the Bank.

Mobile device = a smart phone, tablet, laptop computer, watch, wristband or other similar device that enables a wireless connection to the internet or other mobile phone or data communication network.

Mobile banking services = an app-based electronic service offered by the Bank on the Customer's mobile devices, requiring the use of identifiers.

Online services = eBanking, mobile banking services or telephone services.

Parties = Customer and/or User and the Bank collectively.

Payment account provider = a payment service provider that provides and maintains the Customer's account.

Payment transaction = an event where funds are transferred, withdrawn or placed at the disposal.

Product company = The Bank or a company belonging to the same group which produces the financial service and is responsible for it.

Service request = application, agreement, assignment or other message.

Telephone services = personal telephone service, automated telephone service and web service customer support.

Third party = a company or community, such as an online store or an authority that is not part of the Bank's group.

User = a natural person who represents the Customer and takes care of the Customer's dealings with the Bank. The User acts on behalf of, in the name of and on the account of the Customer. Users are, among others, guardians and trustees who make transactions on behalf of a minor or ward, or Users nominated by corporate customers.

Web meeting = a meeting between the Customer and the Bank in the electronic meeting facility of the eBanking service.

Web payment service = service via which the Customer or the User can pay with his/her identifier when doing business with a third party via the network service.