

Terms and conditions for electronic communication

1. Scope of application

These terms and conditions apply to electronic communication undertaken by the Customer or the User using eBanking or telephone services (hereinafter online services) when the Customer or the User contacts the Bank or when the Bank makes telephone contact with the Customer or the User.

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 agree separately the legal effects of the use of identifiers in connection with the use of the Bank's certification 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 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 personal password for bank identifiers must be stored separately from the customer number and security card, and preferably committed 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 Bank 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, security card or information relating to same, or a telephone fitted with rapid identification, 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. Information on different options for the blocking service can be found on the Bank's website. 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.

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 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 precondition for the use of eBanking is to approve the certificate of the security solution. When the customer or user approves the certificate, the Java-applet of the Bank will be installed to the computer.

The Bank has a right to collect information as follows by using Java-applets or otherwise:

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

The Bank's website www.sampopankki.fi contains additional information about the Java-applets and information collected using the applets.

5.3. Use of information

The Bank has a right to use customer data and transaction information for purposes which are in accordance with the description set out in the Bank's Customer Register.

Information collected by using Java-applets 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

- the usage of the Bank's services during the session will be used for statistic and business development purposes.

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 Requests

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
- 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 has given information regarding safety issues on its website. Descriptions of the hardware and software required under the prevailing threat environment are 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.

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 agreed otherwise.

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. In secure messaging the Customer and the User can also confirm applications and agreements using the identifiers approved by the Bank.

6.4.3 Electronic mailbox

The Bank has a right to send different personal messages and documents to the customer or to the user in electronic form to the electronic

mailbox after the customer has chosen to start to use the electronic mailbox or the customer has given a mandate to the user to receive customer's messages and documents to the user's electronic mailbox.

The Bank's website www.sampopankki.fi contains additional information about the electronic mailbox and the list of messages and documents which will be sent to the electronic mailbox. The Bank has a right to change the before mentioned list as agreed in section 7.1.

Despite the use of the electronic mailbox

- the customer or the user has a right to order the message or the document sent to the electronic mailbox in paper form by paying the service fee based of the price list
- the Bank has always a right to send messages and documents to the customer or to the user in paper form instead of electronic mailbox if it so desires.

6.4.4 Text messages and ordinary e-mail

The Bank has the right to send the Customer or the User

- a text message to remind the Customer or the User to confirm a service request in the online service without the Customer's or the User's consent
- a text message or an ordinary e-mail which contains confidential information only if the Customer or the User has given his/her advance consent.

6.5 Restrictions or interruptions to the service

6.5.1 Planned break of service

- The Bank has the right to interrupt
- telephone services which do not require the use of bank identifiers at any time
- other 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.

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 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 duty 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 damage**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 eBanking

The Bank shall inform customers and users about technical problems and breaks of services relating to eBanking. The information shall be provided on the website and/or on the eBanking log-on page. During breaks of service, 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 is 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 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 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.

6.8.5 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 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 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 one (1) month. 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. The Customer shall be responsible for the service requests which have been made during the validity of this agreement, including during the period of notice. 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, for Finns and Customers and Users who live in Finland irrespective of which country the online services are accessed from
- 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 in respect of this agreement that cannot be resolved through discussion, said dispute shall be resolved in the District Court of Helsinki. Private customers (consumers) are always entitled to institute legal proceedings in the district court of their domicile in Finland.

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

- Advisory Office for Bank Customers, Museokatu 8 A 7 00100 Helsinki, tel. (09) 4056 1230
- The Financial Supervision Authority, Snellmanninkatu 6, P.O. Box 159, 00101 Helsinki, tel. 010 83151.
- The Office of the Data Protection Ombudsman, Albertinkatu 25A, 3rd floor, P.O. Box 315, 00181 Helsinki, tel. 010 366 6700.
- The Consumer Agency and Consumer Ombudsman, Haapaniemenkatu 4 A, 7th floor, P.O. Box 5, 00531 Helsinki, tel. 09-77261.

- The Finnish Communications Regulatory Authority, Itämerenkatu 3 A, P.O. Box 313, 00181 Helsinki, tel. 09-69 661.

Danske Bank A/S, Helsinki Branch, LY 1078693-2. Unioninkatu 22, 00075 SAMPOPANKKI, tel. +358 (0)10 515 15, www.sampopankki.fi. The Ministry of Finance has granted the licence no. VM3/414/2001 to Sampo Bank plc. The Bank is a member of the Federation of Finnish Financial Services, which represents the companies of the financial sector. Copyright Danske Bank A/S. All rights reserved.

Last updated 5/2008.

Definitions

Bank = Sampo Bank plc and its subsidiaries. These companies have been informed on the Bank's web pages.

Bank identifiers = identifier which consists of the personal User ID, a personal password and a security card.

Certification 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.

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-based Internet service provided by the Bank, access to which is controlled by means of an identifier.

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

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.

Online services = eBanking and telephone services geared to private customers.

Parties = Customer and/or User and the Bank, all together.

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 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.