

TERMS AND CONDITIONS FOR ACCESS AGREEMENT – DANSKE EBANKING BUSINESS (EARLIER COMBINED AGREEMENTS)

The terms and conditions applying to Danske eBanking Business agreements are set out below.

Danske eBanking Business is Danske Bank's Internet-based home banking system for small businesses. It allows a user to view and operate the accounts and custody accounts of the account holder.

Payment Services Act

The Payment Services Act applies to payment accounts, that is, accounts opened for the purpose of executing payments. We deviate from the stipulations of the act to the extent allowed, unless these terms and conditions or other agreement concluded with us stipulate otherwise.

Definitions

Account holder means the customer entering into a Danske eBanking Business agreement with us.

User means a person authorised by the account holder to use Danske eBanking Business.

1 Features of Danske eBanking Business

Danske eBanking Business may be used for business purposes only.

Only one person may be registered as user under a Danske eBanking Business agreement. If the account holder wants a new user to be registered under the agreement, the agreement must be amended.

Danske eBanking Business allows the user to

- make enquiries about accounts and custody accounts, including executed and future transactions
- transfer funds to the accounts of the account holder or to accounts of other account holders with Danske Bank, other banks in Denmark or banks in most other countries
- pay electronic payment forms

- trade securities
- communicate electronically with us, allowing us to send information and documents (mail) electronically through Danske eBanking Business

All current features can be viewed in Danske eBanking Business.

1.1 Access to accounts

Danske eBanking Business allows the user to make enquiries about and operate those present and future accounts and custody accounts of the account holder that the user has been or will be assigned authorisation to make enquiries about and operate.

The operation of accounts and custody accounts is governed by the rules applying to the individual accounts.

To make a domestic account transfer, the user must enter the registration number and account number of the payee's account and,

where relevant, the date of the transfer (see the help functions for the individual screens).

To make an international payment, the user must provide the account number/IBAN, SWIFT address and, where relevant, other information about the payee as well as the date of the payment. The Terms and conditions for international payments to and from Denmark and domestic payments in foreign currency to another bank in Denmark as well as the help functions for the individual screens offer additional information on the data required.

We are under no obligation to process orders

- for which there are insufficient funds
- if the data entered is insufficient
- if the account holder or the user suspends payments, is the subject of bankruptcy proceedings, opens negotiations for debt relief or compulsory composition, submits a request for voluntary composition or dies.

The user must enter data for payment forms, funds transfers and securities trades under

the appropriate functions in the system. We cannot execute orders submitted by mail, even if the secure mail function is used.

When the user has entered the data in Danske eBanking Business, the user approves the payment or order with his or her personal password. The time of approval is also the transmission time. Immediately after transmission, the user receives confirmation that we have received the order and that it will be executed on the specified date (see 1.2 Cut-off times, booking date and value date).

1.2 Cut-off times, booking date and value date

A number of cut-off times apply to receipt of orders. See Danske eBanking Business for cut-off times, booking dates and value dates.

1.3 Securities trading

Securities trading through Danske eBanking Business is possible only if the account holder has a custody account with Danske Bank, unless otherwise agreed. The account holder can order an Agreement on custody accounts

and trading in financial instruments through Danske eBanking Business or by contacting us.

The following sub-clauses are relevant only if the account holder wants to trade securities through Danske eBanking Business.

1.3.1 Custody account

The custody account agreement generally offers access to trade in

- bonds
- shares
- unit trust certificates

1.3.2 Investment profile

We recommend setting up an investment profile for the account holder before commencing securities trading. We cannot provide advice on investments or issue recommendations without an investment profile.

To determine the account holder's investment profile, the following factors must be considered:

- The purpose of trading
- The amount to be invested
- The investment horizon
- The type of securities to be traded
- Risk appetite
- The account holder's financial situation
- The account holder's experience with and knowledge of securities types

If the account holder has more than one custody account, we recommend that an investment profile be determined for each account.

1.3.3 How to determine the investment profile

The account holder can determine the investment profile through Danske eBanking Business or by consulting one of our advisers. The adviser determines the investment profile on the basis of the information provided by the account holder.

1.3.4 Questions

We will be happy to answer questions about investment profiles and investment in general.

1.3.5 Execution only

Share, bond and unit trust certificate trades through Danske eBanking Business are execution only trades, which means that no advice is provided nor any recommendations issued. Consequently, we do not check whether the account holder or user has knowledge of or experience with the type of security traded. The account holder and the user are thus not protected by the general rules of the Danish executive order on the protection of investors trading in financial instruments.

1.3.6 Buying and selling securities

Orders for the purchase or sale of Danish securities through Danske eBanking Business can be executed as

- an immediate trade
- an average-price trade
- a market order

The purchase or sale of non-Danish shares can be executed as an immediate trade or on a commission basis.

Immediate trades and average-price trades are made with Danske Bank as seller or buyer.

Market orders and trades executed on a commission basis are executed by us in our own name but for the customer's account. We may, however, act as a party to a trade. Under the Commissions Act, we are then contracting for our own account.

To execute market orders, the account holder must sign the Access agreement – trading on regulated markets – automatic order processing. This agreement allows the user to place purchase and sales orders for shares listed on Nasdaq OMX Copenhagen and Nasdaq OMX Stockholm. The orders are automatically transmitted to SAXESS, the trading system of the two exchanges.

Security trades with us are subject to our Terms and conditions for trading in financial instruments.

Orders can be entered into Danske eBanking Business from 6.00am to 12.00 midnight.

We consider an immediate trade to have been concluded when the user has accepted the price and submitted the order to us through Danske eBanking Business.

Immediate trades in selected shares and bonds through Danske eBanking Business may be executed from Monday to Friday during the following periods (CET):

Denmark	9.00am	to	10.00pm
USA	3.30pm	to	10.00pm
Sweden	9.30am	to	5.30pm
Norway	10.00am	to	4.00pm
Finland	9.30am	to	4.30pm
Switzerland	9.00am	to	5.00pm
Germany	9.00am	to	8.00pm
Other European exchanges	9.00am	to	5.30pm

Trades executed on a commission basis are, if possible, executed between 9.00am and 10.00pm (CET), depending on the opening hours of the relevant exchange.

A confirmation is sent to the account holder after execution.

1.3.7 Information in Danske eBanking Business

Danske eBanking Business contains a number of research reports, calculations, assessments and estimates prepared by us. We strive to ensure that this information is correct and reliable. We do not, however, assume any liability for the accuracy and completeness of the information.

Moreover, Danske eBanking contains information obtained from Danske Bank's business partners. We have selected these business partners carefully, but assume no liability for the information passed on.

Similarly, we do not assume any liability for losses incurred as a result of actions taken on the basis of information provided in Danske eBanking Business. Such information has been prepared exclusively for guidance and does not constitute and should not be construed as an invitation or offer to buy or sell securities or

foreign exchange or enter into contracts on financial instruments. The information, research reports, calculations, assessments and estimates provided in Danske eBanking Business are not a substitute for own judgement about whether or not to enter into any such transactions.

1.4 Amount limits

There is a limit to the maximum value of payments and cash transfers the user can make each day. Information on applicable limits is available in Danske eBanking Business and from our branches.

A limit also applies to the value of each securities transaction. Information on the limits applying to share and bond trading is also available in Danske eBanking and from our branches.

2 Terms and conditions for use

When an agreement on Danske eBanking Business is concluded, the user authorised by the account holder can make account

enquiries and operate (some of) the account holder's accounts with Danske Bank through Danske eBanking Business.

The user accesses Danske eBanking Business using the security solution(s) chosen. In practice, this means, for example, that the user can create a transfer from one account to another and use his or her personal password to approve it. Transactions made with the user's personal password are binding on the account holder as if the account holder had signed a printed agreement.

2.1 Security solutions

The user can choose between two security solutions: e-Safekey® or ActivCard (see 18 Technical requirements).

2.1.1 e-Safekey®

The e-Safekey® security solution consists of three elements:

- A user ID provided to the user either by the local branch or by separate letter
- The user's personal password

- The user's personal user ID, which is saved as a file on the user's computer

The e-Safekey® security solution includes a feature ensuring that the user can access Danske eBanking Business only from the computer to which e-Safekey® is locked. The user can lock e-Safekey® to several computers, however.

The user must not

- disclose his or her personal password or user ID to others
- copy the personal user ID to a computer over which the user does not have full control
- write down the password and keep it near the computer. The user should choose a password that is easy to remember

When the user communicates with us, we may ask the user to state the original user ID. We will never, however, ask the user to disclose the personal password or send us the file with the personal user ID.

If the user or the account holder suspects that somebody else may know the personal password or user ID, we must be contacted immediately (see 19 Blocking and notification in case of irregularities and unauthorised use).

2.1.2 ActivCard

The ActivCard security solution consists of three elements:

- A user ID provided to the user either by a branch or by separate letter.
- The user's personal password
- An ActivCard, which is a type of pocket calculator that generates one-time passwords

The user must not

- disclose his or her personal password, ActivCard PIN or the ActivCard itself to others
- write down the password and PIN and store them with the ActivCard. The user should choose a password that is easy to remember

When the user communicates with us, we may ask the user to state the user ID, but will never ask the user to disclose the personal password.

The user should be particularly attentive to security risks when using the ActivCard solution on computers over which the user does not have full control.

If the user or the account holder suspects that somebody else may know the user's personal password or have access to the user's ActivCard, we must be contacted immediately (see 19 Blocking and notification in case of irregularities and unauthorised use).

3 Use of Danske eBanking Business

Using the personal password in Danske eBanking Business is as legally binding as a signature on a printed document. Danske eBanking Business and the user's security solution(s) are thus considered personal and may be used by the user only.

The user must store information about the security solution in such a way that others will not have access to this data.

4 Computer security

To avoid unauthorised use of Danske eBanking Business, it is important that the user and the account holder protect the computer by always applying the latest software updates, antivirus software and a firewall. See www.danskebank.dk for more advice on security.

5 Check of account entries

When a transaction has been executed, it will appear on the list of account entries in Danske eBanking Business. The list of account entries displays all transactions executed during a period of up to 13 months. Each quarter, the user can see the fees paid for the past month. In addition, we regularly send account and custody account statements as prescribed by the terms and conditions governing the individual accounts.

Note that there may be transactions that have not yet been finally registered on the account or custody account.

The account holder and the user are obliged regularly to check entries in the account holder's accounts and custody accounts. If the list contains transactions that they do not believe they have authorised, they must contact us as soon as possible and not later than one month after the amount was charged to the account.

6 Revocation

The account holder and the user may revoke account transfers and payment of payment forms until the last banking day before the requested execution date.

Payments via Betalingservice (direct debit) may be revoked until the seventh day of the month of payment. If this is not a banking day, the deadline is the preceding banking day.

See Questions & Answers in Danske eBanking Business for guidelines on how to revoke a payment.

Orders for average-price trades (not immediate trades) may be cancelled on the same day as they are placed, while orders for future securities trades may be cancelled until the day before the execution date. See the help functions in Danske eBanking Business for guidelines on how to revoke a securities trade in due time.

The user/account holder must contact us to revoke other order types.

7 Account holder's liability

The following stipulations apply to transactions made with the user's personal password:

- The account holder is liable for losses up to DKK 1,100 if the user's personal password has been subject to unauthorised use.

- The account holder is liable for losses up to DKK 8,000 (including excess) if we can prove that the user's personal password was used and that the user did not contact us as soon as possible after discovering that another person had obtained the user's personal password. The same applies if the user informed the unauthorised user of the user's password but is not fully liable for the loss under Danish law, or if, through gross negligence, the user made unauthorised use possible.
- The account holder is liable for the full loss if we can prove that the user disclosed his or her personal password to the unauthorised user and that the user realised, or ought to have realised, that there was a risk of unauthorised use.
- The account holder is also liable for the full loss if the user has committed fraud or has deliberately omitted to protect his or her personal password (see 2) or block the agreement (see 19).

- The account holder is not liable for losses arising after we have been asked to block the agreement.

Read more about liability in sections 62, 63 and 64 of the Payment Services Act (excerpt at the end of this document).

8 Danske Bank's liability

Danske Bank is liable for the tardy or defective performance of its contractual obligations resulting from error or negligence, unless otherwise stipulated in 7 Account holder's liability.

Even in areas of increased liability, Danske Bank is not liable for losses arising from

- breakdown of or lack of access to IT systems or damage to data in these systems due to any of the factors listed below and regardless of whether Danske Bank or a third-party supplier is responsible for the operation of these systems
- power failure or a breakdown of Danske Bank's telecommunications, legislative or

administrative intervention, acts of God, war, revolution, civil unrest, sabotage, terrorism or vandalism (including computer virus attacks or hacking)

- strikes, lockouts, boycotts or picketing, regardless of whether Danske Bank or its organisation is itself a party to or has started such conflict and regardless of its cause (this also applies if the conflict affects only part of Danske Bank)
- other circumstances beyond Danske Bank's control

Danske Bank is not exempt from liability if

- Danske Bank ought to have foreseen the cause of the loss when the agreement was concluded or ought to have avoided or overcome the cause of the loss
- under Danish law, Danske Bank is liable for the cause of the loss under any circumstances

Where Danske Bank is liable to pay damages, it is liable, in accordance with the ordinary rules of liability, for direct losses attributable to errors it has committed. Other than that,

Danske Bank's liability is limited to the remedying of defects. Further liability cannot be asserted, not even liability for indirect consequences or resulting harmful effects.

The above stipulations on liability replace those of Section 68 of the Payment Services Act, which thus do not apply.

9 Use of Danske eBanking Business

The services received through Danske eBanking Business, including price information, are exclusively for the account holder's and the user's own use. The account holder and the user are not allowed to pass on this information to others, with or without consideration, without our written consent.

10 Complaints

The account holder should always contact the local branch in case of a disagreement concerning the business relationship with us to make sure that such disagreement is not based on a misunderstanding. The account

holder can also call us on tel. +45 70 123 456 (open seven days a week).

If the account holder still disagrees or is not satisfied with the outcome of the complaint, the account holder may write to our Legal department, which is in charge of handling customer complaints.

The address is

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

11 Changes to terms and conditions and system features

We reserve the right to amend these terms and conditions and to adjust system features without notice. We will announce changes in the Danish daily press, by letter or electronically, for example, by e-mail or a message in Danske eBanking Business.

If we significantly curtail the features of the system, we will announce this by letter or electronically through Danske eBanking Business at one month's notice.

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

If we are informed that the account holder does not want to be bound by the new conditions, the agreement will terminate when the new conditions take effect.

12 Termination

The account holder may terminate the Danske eBanking Business agreement in writing at any time without notice.

We may terminate the account holder's Danske eBanking Business agreement at one

month's notice. In the event of default, we are entitled to terminate it without notice, however.

Orders and agreements entered into prior to termination will be executed (see, however, 1.1).

13 Costs associated with access and use

An updated list of charges is available in Danske eBanking Business specifying the most common fees for use of Danske eBanking Business.

Transaction fees are charged to the accounts used for the transactions.

If the account holder requests supplementary or more frequent information than agreed under the Danske eBanking Business agreement, we reserve the right to charge a fee for providing such information.

We may charge fees for the payments the account holder makes from an account and for

providing the account holder with details about payments made.

We may also charge a fee for help to recover funds transferred to an account by mistake because the user stated a wrong unique identifier.

14 Assessment of customers

An offer for Danske eBanking Business is subject to an individual assessment of our business relationship with the account holder. We reserve the right to decline entering into an agreement on Danske eBanking Business with the account holder and to decline acceptance of a proposed user.

15 Use, storage and passing on of customer data and information about purchases, etc.

When the user uses Danske eBanking Business, we register the user ID, the payer's and payees' account numbers and the amount and date of the transaction.

If the system is used for transfers, we forward information on amount and transaction date as well as any message from the user to the payee. Data is transmitted through the payee's bank and its data and settlement centre.

The information is stored with the payee's bank and Danske Bank. The information is used by the banks for bookkeeping purposes, account statements and subsequent correction of errors, if any.

The information is passed on only if required by Danish law or if it is needed for legal actions arising out of the use of the system.

The information is kept on file for the year of registration and the following five years.

16 User's securities trading

If the account holder requires the user to trade securities for the account of the account holder, the account holder is responsible for ensuring that the user knows relevant parts of the account holder's investment profile. The

account holder/user must also be aware that the account holder may incur losses on investments.

The Information about trading in financial instruments publication includes information about investment profile, security types and investment choices. We recommend that the account holder/user read that publication prior to trading.

The account holder/user must also note the special tax rules on securities trading and the rules on inside information. More information is provided by the help screens in Danske eBanking Business and in the Information about trading in financial instruments publication.

17 Automatic registration for receipt of documents (mail) in electronic mailbox

These conditions apply only if the account holder does not have e-Boks.

On entering into a Danske eBanking Business agreement, the account holder is automatically registered for receipt of documents (mail) from us in the electronic mailbox.

The account holder receives electronic documents from us to the same extent and with the same legal validity as printed documents. To receive documents from us electronically, the account holder must have access to Danske eBanking Business and have authorised the user to use the system. The user has access to the electronic mailbox.

17.1 Documents received electronically

The account holder receives all documents that we send electronically in the electronic mailbox. The account holder thus no longer receives the printed documents.

Account statements, confirmations, payment advices and other statements are examples of documents that the account holder receives electronically.

We regularly add new documents to the range we send electronically. The account holder does not receive separate notification each time we send a new type of document in electronic form and stop sending a printed version of the document.

17.2 Storage etc.

We store documents sent electronically to the electronic mailbox for at least five years. The documents will be deleted, however, if the account holder switches to another bank or otherwise terminates the Danske eBanking Business agreement.

If the account holder wants to store the documents, the user can print them or save them on a computer. We recommend that the account holder and the user agree on the method of storing and on the computer to be used for storage.

17.3 Responsibility and liability

17.3.1 Account holder

The user is responsible, on behalf of the account holder, for opening and checking the documents that we send electronically. The user should check the documents carefully in the same manner as the user would check printed documents. Moreover, the account holder is responsible and liable in the same way as if the account holder had received the printed version of the documents by letter.

If the user does not have access to Danske eBanking Business for a while, the account holder must immediately inform us whether the account holder wants to receive printed documents by mail instead.

17.3.2 Danske Bank

Danske Bank's liability is governed by the rules on liability stipulated in 8.

We reserve the right to send documents normally sent electronically in printed versions by mail.

17.4 Deregistration

The account holder and the user may deregister for receipt of documents electronically at any time by giving us written notification. The user can also do so through Danske eBanking Business.

Note that it may take up to 12 days from we receive the notification of deregistration until the change takes effect.

17.5 Termination

If the Danske eBanking Business agreement is terminated – irrespective of the reason – the account holder will no longer receive documents in the electronic mailbox.

17.6 Electronic payment information

If the account holder, now or later, chooses to pay bills through Betalingservice (direct debit), the registration for receipt of documents (mail) from us in the electronic mailbox also covers the payment information.

We will then send future payment summaries to the account holder's electronic mailbox only. The user receives electronic documents from us on behalf of the account holder to the same extent and with the same legal validity as printed documents.

17.6.1 Storage

The electronic payment information will be accessible in the standard module of Danske eBanking Business during the month in which the payment is effected and the next 13 months.

The electronic payment information is stored in the electronic mailbox according to the guidelines set out in 17.2.

If the account holder wants to store electronic payment information, the user can save it on a computer.

17.6.2 Printed payment summaries

If at some point the account holder wants to receive payment information (Betalingsservice payment summaries) as printed documents again, the account holder must deregister for

receipt of electronic mail and will subsequently receive printed documents from us by letter.

If the account holder wants to deregister for receipt of electronic payment summaries and wants to be sure that the payment information is sent in printed form from the requested month, the account holder must deregister at least 12 days before the first of the month from which the change is to take effect.

17.6.3 Change of bank

If the account holder switches to another bank, the account holder must arrange with the new bank how to receive payment information.

17.6.4 Special conditions

The General conditions for Betalingsservice debtors applicable as from 1 November 2009 apply to the registration for Betalingsservice. The account holder should pay particular attention to clause 6 Electronic payment information.

18 Technical requirements

To use electronic services, the account holder needs a web browser and Internet access. Read more about how to set up your browser on www.danskebank.dk.

The e-Safekey[®] security solution is compatible only with Internet Explorer for Windows. If another operating system such as Mac, or another browser, is used, the user must opt for the ActivCard security solution.

19 Blocking and notification in case of irregularities and unauthorised use

The account holder and the user can block the Danske eBanking Business agreement 24 hours a day by calling our blocking service on tel. +45 70 20 70 20.

We will subsequently send written confirmation of the blocking, specifying the time when we received the request for blocking.

For security reasons, the agreement will automatically be blocked if the user has not activated it within two months of the signing of the agreement.

The account holder and the user must inform us immediately if they discover or suspect irregularities or unauthorised use of the Danske eBanking Business agreement.

We reserve the right to block the agreement without notice if we discover or suspect irregularities or unauthorised use of your agreement.

The user/account holder must contact Customer Service to cancel the blocking.

20 New copies of these terms and conditions

Should the account holder and the user need an additional copy of these terms and conditions, they can either request one from the account holder's branch or download it from www.danskebank.dk. We will charge a fee for sending printed copies.

21 Telephone numbers and opening hours

Customer Support

Customer Support can answer questions about installation and use of Danske eBanking Business. Customer Support can be reached on tel. +45 70 10 55 01 - the opening hours (CET) are

- Monday–Thursday: 8.00am–11.00pm
- Friday: 8.00am–6.00pm
- Saturday: 10.00am–6.00pm
- Sunday: 10.00am–11.00pm

Calls to Customer Support are charged at normal call charges. Customer Support can also be contacted in writing.

Business hours

Danske eBanking Business is open 24 hours a day, 365 days a year.

Payment Services Act

Rules on liability

62.-(1) The payer's provider is liable to the payer for any loss incurred due to the unauthorised use by any third party of a payment instrument unless otherwise provided in (2)-(6) hereof. The payer is only liable under (2)-(6) hereof if the transaction was accurately recorded and entered in the accounts. In case of unauthorised use of a payment instrument, the payer's provider shall immediately reimburse the payer with the amount.

However, the payer is liable without limitation with respect to any loss incurred due to the payer acting fraudulently or with intent failing to fulfil his obligations under section 59.

(2) Except where more extensive liability follows from (3) or (6) hereof, the payer is liable for an amount up to DKK 1,100 for any loss incurred due to the unauthorised use by a third party of the payment instrument where the payment instrument's personalised security feature was used.

(3) Except where more extensive liability follows from (6) hereof, the payer is liable for an amount up to DKK 8,000 for any loss incurred due to the unauthorised use by a third party of the payment instrument provided that the payer's provider proves that the payment instrument's personalised security feature was used, and

(i) that the payer failed to notify the payer's provider without undue delay on becoming aware of the loss of the payment instrument, or of the personalised security feature having come to the knowledge of the unauthorised person;

(ii) that the payer passed the personalised security feature on to the person making the unauthorised use without this falling within the scope of (6) hereof; or

(iii) that the payer facilitated the unauthorised use by gross recklessness.

(4) The payer is liable for an amount up to DKK 8,000 for any loss incurred due to the unauthorised use by a third party of the payment instrument where the payment instrument was read physically or electronically and the unauthorised person in

connection therewith used a false signature, and the payer's provider proves

(i) that the payer or a person to whom the payer entrusted the payment instrument failed to notify the payer's provider without undue delay on becoming aware of the loss of the payment instrument; or

(ii) that the payer or a person to whom the payer entrusted the payment instrument facilitated the unauthorised use by gross recklessness.

(5) Where the payer is liable under (3) and (4) hereof, the payer's total liability cannot exceed DKK 8,000.

(6) The payer is liable without limitation with respect to any loss incurred due to the unauthorised use by a third party of the payment instrument where the payment instrument's personalised security feature was used and the payer's provider proves that the payer disclosed the personalised security feature to the person making the unauthorised use, and that the circumstances were such that the payer knew or ought to have known that there was a risk of abuse.

(7) Notwithstanding the provisions of (2)-(6) hereof, the payer's provider is liable for any unauthorised use after the provider was notified that the payment instrument had been lost, that the personalised security feature had come to the knowledge of an unauthorised person, or that the payer required the payment instrument to be blocked for any other reason.

(8) Notwithstanding the provisions of (2)-(6) hereof, the payer's provider is liable for any unauthorised use if the provider did not provide appropriate means, cf. section 60(1)(ii).

(9) Moreover, notwithstanding the provisions of (2)-(6) hereof, the payer's provider is liable if the payee knew or ought to know that the use of the payment instrument was unauthorised.

(10) It may be agreed that (1)-(6) hereof shall not apply to micro-payment instruments used anonymously, or where the nature of the micro-payment instrument makes the payer's provider unable to prove that the payment transaction was authorised. It may furthermore be agreed that (7) and (8) hereof shall not apply to micro-payment instruments

where the nature of the payment instrument makes it impossible to block its use.

(11) The provisions of (1)-(6) hereof apply to e-money except where the payer's provider of e-money is unable to block the payment account or the payment instrument.

63. Contestations concerning unauthorised or incorrectly executed payment transactions must be received by the provider as soon as possible and not later than 13 months after the debit date of the relevant payment transaction. Contestations from the payee must be received within 13 months of the credit date. Where the provider has not provided information or made information available under Part 5, the deadline is calculated from the date on which the provider provided information or made information available.

64.-(1) The provider has the burden of proof with respect to a payment transaction being accurately recorded and entered in the accounts and not affected by a technical breakdown or some other deficiency. In

connection with the use of a payment instrument, the provider furthermore has to prove that the payment instrument's personalised security feature was used in connection with the payment transaction. The recorded use of a payment instrument is not in itself proof that the payer authorised the transaction, that the payer acted fraudulently or failed to fulfil his obligations, cf. section 59. (2) It may be agreed that (1) hereof shall not apply to micro-payment instruments used anonymously, or where the nature of the payment instrument makes the provider unable to prove that the payment transaction was authorised.