

Terms and Conditions Business Online

20 March 2011



branch of Danske Bank

Contents

Introduction	4
Part 1 – Business Online – general description	4
1. Modules and services	4
2. Transactions	4
3. Registered accounts	4
3.1. Registered accounts within the Danske Bank Group	4
3.2. Registered accounts managed via SWIFT	4
4. Unregistered accounts	4
5. Cheque payments	5
6. Requests	5
6.1. Submission of requests	5
6.2. Binding requests	5
6.3. Retention of requests	5
7. Use of electronic communications - eArchive	5
7.1. Who has access to the documents	6
7.2. Archiving	6
7.3. Deregistering eArchive	6
7.4. Termination	6
8. User Authorisations for Business Online	6
8.1. Administrator privileges	6
8.2. Agreement Administrator	7
8.3. User Administrator	7
8.4. Agreement Information	7
8.5. PIN and blocking	7
8.6. Viewing documents	7
8.7. Access to accounts	7
8.8. Transaction types	8
8.9. Confidential payments	8
8.10. Changing Business Online User Authorisations	8
8.11. Revoking Business Online User Authorisations	8
9. Other mandates in Business Online	9
9.1. Third-party mandates granted to the company	9
9.2. Authorisation to buy/sell foreign exchange and securities	9
9.3. Trade Finance Authorisation in Business Online	9
10. Authorisation types	10
10.1. Authorisation types	10
10.2. Separate authorisation	10
10.3. Two persons jointly (A authorisation)	10
10.4. Two persons jointly (B authorisation)	10
10.5. Two persons jointly (C authorisation)	10
11. Customer support	10
Part 2 – Business Online – security system	11
12. Technical issues	11
12.1. Transmission and access	11
12.2. Distribution, control and storage of software	11
12.3. Data security	12
13. Acquiring a user ID and a temporary PIN	12
13.1. Security registration and key generation	12
13.2. Password	12
13.3. Changing the password	13

13.4.	Deregistering users/keys	13
13.5.	Misuse or risk of misuse of key	13
14.	Ban on encryption	13
Part 3 – Contractual aspects		13
15.	For business purposes only	13
16.	Changing Business Online	13
17.	Changes to service and support	13
18.	Responsibilities and liability	13
18.1.	The company's responsibilities	13
18.2.	The Bank's responsibilities	14
19.	Other terms and conditions	15
19.1.	Structure of the Business Online Agreement	15
19.2.	Prices	15
19.3.	Other amendments to Business Online agreements	15
19.4.	Assignment, transfer and third parties	15
20.	Termination and breach	15
21.	Choice of law and legal venue	16
22.	Definitions and glossary	16

Introduction

Business Online is Fokus Bank's Internet-based office-banking system, which provides access to account information, payments and other banking transactions requested by the company.

The Terms and Conditions for Business Online include a description of the system.

Part 1 – describes the options available in Business Online and how to use the system.

Part 2 – describes the security requirements for Business Online users.

Part 3 – describes the contractual aspects of connecting to Business Online.

Part 1 – Business Online – general description

1. Modules and services

Business Online comprises separate modules and services.

The Module Description comprises a description of the modules and services available via the company's Access Agreement.

2. Transactions

Business Online allows the company to, for example, make payments and queries on balances and movements in accounts registered in Business Online via the Access Agreement. Payments and queries are jointly referred to as transactions.

3. Registered accounts

Accounts must be registered in Business Online before a company can make transactions via Business Online.

Accounts are registered via the Access Agreement.

3.1. Registered accounts within the Danske Bank Group

Accounts opened with Fokus Bank and affiliates and divisions of the Bank under this agreement are accounts within the Danske Bank Group.

The following accounts within the Danske Bank Group can be registered in Business Online:

- Accounts held by the company and opened in the name of the company
- Accounts held by third parties, including subsidiaries, provided that the third party or subsidiary has issued a third-party mandate to the company authorising the latter to act on behalf of the third party or subsidiary

Registered accounts within the Danske Bank Group can also be managed via SWIFT MT101 or MT940, see section 3.2.

3.2. Registered accounts managed via SWIFT

Accounts opened with banks outside the Danske Bank Group, and accounts within the Group which the company wishes to use for transactions via SWIFT MT101 or MT940, can also be registered in Business Online via the Access Agreement. The company may register both its own accounts and third-party accounts. The company or third party must conclude an agreement with the account-holding bank concerning payment requests via MT101 or an agreement on Balance Reporting via MT940.

Third-party accounts can only be registered if the third party has issued a mandate to the company.

4. Unregistered accounts

If accounts held by the company and/or a third party are not registered in Business

Online, it is only possible to make payments into these accounts. It is not possible to inquire about or make payments from unregistered accounts.

5. Cheque payments

The company may make payments by issuing a foreign cheque drawn on a registered account within the Danske Bank Group.

If the company and/or a third party has an agreement concerning payment requests via MT101, cheques can also be drawn on registered accounts outside the Danske Bank Group, provided that this option is included in the agreement between the company and/or third party and the bank outside the Danske Bank Group.

Issued cheques are regarded as banker's cheques, and the amounts are debited from the accounts on the date of issue.

The company may have the proceeds of uncashed cheques deposited in registered accounts.

If the proceeds from uncashed cheques are to be credited to the company's or a third-party's account, the company or third party must pledge to indemnify the Bank if a cheque is subsequently cashed.

6. Requests

A request by the company or its users for a transaction in Business Online, for example a payment, is called an electronic request.

6.1. Submission of requests

When a user submits an electronic request on behalf of the company and/or a third party, the Bank sends an electronic receipt. The moment we have confirmed receipt of the request, the risk in relation to

its being carried out in accordance with the instructions passes to the Bank.

6.2. Binding requests

Requests carried out in accordance with the instructions in the electronic request are binding on the company.

Consequently, the Bank cannot reverse payments, trades in foreign exchange or securities or other transactions, including cheque issuance, finalised in accordance with the request.

6.3. Retention of requests

We retain electronic requests for at least ten years. During this period, the company and/or third party whose account is debited may obtain a hardcopy of the request against payment of the fee charged by the Bank for extraordinary assistance.

7. Use of electronic communications - eArchive

The Bank may send all information and messages as electronic documents to eArchive within Business Online.

Information and messages that the company has received in electronic form will have the same legal effect as if the documents had been sent by ordinary mail.

If the company is a customer of one or more of the Danske Bank Group's other companies, and they send documents to the company electronically, the Group may also send them to Business Online in electronic form.

The types and number of electronic documents that the company receives in eArchive will be extended on an ongoing basis. The company will be notified in Business Online every time a new type of document from the Bank becomes

available in electronic form in eArchive. The Bank may however decide at any time to send a document by ordinary mail. Where possible, the Bank will give notice of this in Business Online.

7.1. Who has access to the documents

Users with query access to the account(s) have access to the documents in eArchive linked to the specific account(s).

7.2. Archiving

The Bank will retain the electronic documents in eArchive for the current year plus five years as a minimum. The company should be aware, however, that the documents will be deleted if the company deregisters an account, changes customer number or cancels Business Online. In such cases we recommend that the company copies the documents itself.

If the company needs to keep the documents for a longer period than the Bank allows via Business Online, it should copy the documents for its own files.

7.3. Deregistering eArchive

If the company does not wish to receive documents in eArchive, it must notify the Bank of this. Subject to agreement, the Bank may forward documents by ordinary mail, against payment of a fee.

7.4. Termination

If the company's Business Online agreement is cancelled, its registration number changes or accounts are removed from its Business Online agreement, it will no longer be able to receive or retrieve electronic documents from eArchive either. See section 7.2 Archiving, etc.

8. User Authorisations for Business Online

All users performing transactions in Business Online on behalf of the company or a third party must be duly authorised to do so by the company. This authorisation is created via the Bank's User Authorisation Business Online.

If a third party has signed a mandate to the company, the company may delegate this mandate to a user. This is done via the User Authorisation in Business Online.

When creating a User Authorisation for Business Online, the company must obtain the user's consent before passing on his or her national identity number to the Bank.

If a user needs to have cash access, e.g. to carry out transactions via the cashier's desk, the company must sign the Mandate – Corporate customers form.

8.1. Administrator privileges

Companies with access to the Administrator module must consider whether users are to be granted administrator privileges. The following administrator privileges may be granted:

- Agreement Administrator
- User Administrator
- Agreement Information
- PIN and blocking

For users granted Agreement and/or User Administrator privileges, the company must decide what level of authorisation the user is to have. The following may be granted:

- Separate authorisation
- Two persons jointly (A authorisation).

For a description of our authorisation types, see section 10.

8.2. Agreement Administrator

A user who is granted Agreement Administrator privileges will be able to

- create, modify and delete Agreement Administrator privileges
- create, modify and delete User Administrator privileges – see section 8.3
- create and delete Agreement Information privileges – see section 8.4
- create and delete user privileges in relation to PINs and blocking – see section 8.5

Agreement Administrators may grant these privileges to themselves and others.

When a user with Agreement Administrator privileges creates or modifies a user with Agreement Administrator privileges, a User Authorisation with a signature field is generated in Business Online. The User Authorisation is accessible in eArchive to users with Agreement Information privileges. The User Authorisation must be signed by the company and sent to the Bank. In other cases, the user accepts and signs using his or her digital signature.

Users with Agreement Administrator privileges also have User Administrator privileges.

8.3. User Administrator

A user who is granted User Administrator privileges will be able to

- create and modify users, including giving users access to modules, accounts, authorisations and transaction types
- create and modify user master data

- delete all user details, including master data.

User Administrators may grant these privileges to themselves and others.

8.4. Agreement Information

Users with Agreement Information privileges can access the users on the agreement and view their individual privileges (including master data, modules, administrator privileges, access to accounts and payment access).

Users also have access to selected documents shown in Business Online.

8.5. PIN and blocking

If the company grants a user PIN and blocking rights, the user will be able to

- order PINs for users
- block and unblock users.

8.6. Viewing documents

A user may view a number of documents in Business Online.

The rights and authorisations granted to the individual user determine which documents the user can view in Business Online.

A user will, for instance, be able to view his or her individual User Authorisation in Business Online.

8.7. Access to accounts

For each user, the company must state which accounts the user may inquire about and/or make payments from. If the company authorises a user to make payments from an account, the user is granted access to the transaction types determined by the company.

For each account that the user is granted access to, the user's authorisation must be stated. The following authorisations are available at account level:

- Separate authorisation
- Two persons jointly (A authorisation)
- Two persons jointly (B authorisation)
- Two persons jointly (C authorisation)

The various authorisations granted by the Bank are described in section 10.

Note that the authorisation granted at account level is reflected in all Business Online agreements under which the account is registered.

8.8. Transaction types

For each user, the company must state which transaction types the user is to have access to:

- Payments between registered accounts in the same country within the Danske Bank Group
- Payment requests via SWIFT MT101
- Payments to unregistered accounts within or outside the Danske Bank Group, including cheque payments
- Cross-border payments accounts within or outside the Danske Bank Group

Furthermore, the company must state whether the user is to be authorised to create and approve, or only to create, the payments selected. If the user is authorised to both create and approve payments, the relevant authorisations for each transaction type must also be stated. The following authorisations are available at transaction level:

- Separate authorisation
- Two persons jointly (A authorisation)

The various authorisations granted by the Bank are described in section 10.

In general, the selected authorisation is used for all payments within each payment type. If the company has selected a more restrictive authorisation at account level, this authorisation will apply for payments to unregistered accounts and cross-border payments. Note that if the user has not been granted any authorisation at account level, this is also regarded as a restriction.

8.9. Confidential payments

The company must state whether the user is authorised to make confidential payments. Confidential payments include payments such as wages and salaries, which may only be viewed, created or approved by users with these privileges.

Users are authorised to make confidential payments within the transaction types to which they have been granted access.

Note that no distinction is made between confidential and non-confidential payments in connection with account queries.

8.10. Changing Business Online User Authorisations

If the company wishes to extend or limit a user's access to Business Online, a new User Authorisation for Business Online must be issued, replacing the previous one.

If the change relates to the user's authorisations at account level, the company and/or third party must also sign an account mandate.

Note that a user's authorisation in Business Online may be affected if the company issues a Mandate – Corporate customers.

8.11. Revoking Business Online User Authorisations

User Authorisations for Business Online remain in force until revoked by the

company in writing. Authorisations may also be revoked by telephone, but this must always be followed up by immediate written confirmation. The user's access to act on behalf on the company via Business Online is blocked after the telephone call.

When the Bank has received notice of revocation, we will send written confirmation that the user number and key have been deleted in its systems.

If the company terminates the entire Business Online Access Agreement, the Bank construes this as revocation of all User Authorisations granted under the agreement.

If the company and/or a third party has granted the user an account mandate, this mandate must be revoked separately. It is not sufficient for the company merely to revoke the Business Online user authorisation.

9. Other mandates in Business Online

9.1. Third-party mandates granted to the company

If the company wishes to make transactions on third-party accounts with the Danske Bank Group, the third party must sign the Bank's third-party mandate form.

If account queries are to be possible on third-party accounts outside the Danske Bank Group, an agreement stating that the Danske Bank Group may receive data about the third party's external account(s) must be submitted to the Bank.

If the company is to make payments from the third party's accounts outside the Danske Bank Group, an agreement stating

that the company may send payment instructions to the third party's bank(s) via the Danske Bank Group must be submitted to the Bank.

The Bank registers the third-party accounts in Business Online via the company's Access Agreement.

9.2. Authorisation to buy/sell foreign exchange and securities

If a user is to have access to information, be able to view trade positions and buy and sell foreign exchange spot and forward, as well as to buy and sell Norwegian and foreign shares, bonds and investment certificates, the user must have access to one or more Markets Online modules. Access to buy and sell foreign exchange spot and forward and to buy and sell shares, bonds and investment certificates also requires that the company grants the user Currency trading and/or Securities trading authorisations. These authorisation only authorise the user to perform transactions on behalf of the company via Markets Online.

All transactions relating to purchase and sale of foreign exchange spot and forward are subject to the provisions of the framework agreement on netting and final settlement of trades concluded between the company and Fokus Bank.

The User Authorisation Business Online must state the accounts and custody accounts that the user is authorised to inquire about or trade in.

9.3. Trade Finance Authorisation in Business Online

If a user is to be able to issue letters of credit, collect debt and/or issue guarantees, the company must register the user for the Trade Finance module and

sign the Connection to/Modification of the Trade Finance Module in Business Online agreement. In this connection, the company must state whether the user is to have access to

- letters of credit (exports and/or imports)
- debt collection (exports and/or imports)
- guarantees.

Furthermore, the company must state whether the user is to have access to

- create and inquire
- create and approve – two persons jointly (A authorisation)
- create and approve – separately (Separate authorisation)

10. Authorisation types

10.1. Authorisation types

Fokus Bank operates with the following authorisation types:

- Separate authorisation
- Two persons jointly (A authorisation)
- Two persons jointly (B authorisation)
- Two persons jointly (C authorisation)

These authorisations allow the company to specify which users may, separately or jointly, approve a payment or request. The authorisations are described in the following.

10.2. Separate authorisation

When requests or payments are created or changed by a user with this authorisation, they are automatically deemed to have been approved by the user. Users with this authorisation can also approve requests or payments entered by users with all other authorisation types.

10.3. Two persons jointly (A authorisation)

When requests or payments are created by a user with an A authorisation, they are automatically approved by this user (1st approval). Further approval (2nd approval) by a user with Separate, A, B or C authorisation is required.

Users with A authorisations rank equally, and the order of approval is therefore of no consequence.

10.4. Two persons jointly (B authorisation)

When requests or payments are created by a user with a B authorisation, they are automatically approved by this user (1st approval). Further approval (2nd approval) by a user with Separate, A or C authorisation is required. Two users with B authorisations cannot jointly approve a payment.

10.5. Two persons jointly (C authorisation)

When requests or payments are created by a user with a C authorisation, they are automatically approved by this user (1st approval).

Further approval (2nd approval) by a user with Separate, A or B authorisation is required. Two users with C authorisations cannot jointly approve a payment.

11. Customer support

The Bank provides support and service to the company. Support and service includes

- user administration
- on-site support
- telephone support
- Internet-based support functions

User administration often includes establishment of Access Agreements and authorisations, adjustment of the company's and its users' access to the

various support and service features, deletion and blocking of users, ordering of temporary PINs and registration of modifications to authorisations, etc.

On-site support may include installation of and training in Business Online, as well as related troubleshooting. Troubleshooting may result in adaptation and/or modification of the computer set-up and the company's IT systems, including modification of registration databases, installation of routers, firewalls and proxy servers, internal security systems and other software and hardware modifications. Installation and troubleshooting take place in cooperation with the company's IT department and at the risk of the company.

Telephone support may include training, user instruction, troubleshooting assistance and guidance in relation to modification. Telephone support in connection with installation, set-up, training and troubleshooting, etc. of Business Online is provided in cooperation with the company's IT department and at the risk of the company.

Internet-based support may include training, user instruction, troubleshooting assistance and guidance in relation to modifications. Internet-based support is provided in cooperation with the company's IT department and at the risk of the company.

Part 2 – Business Online – security system

12. Technical issues

12.1. Transmission and access

In order to use Business Online, the company must establish a data

communication link with Fokus Bank. The company must establish and bear the costs related to the link and must purchase, install, set up and maintain the required IT equipment.

Likewise, the company must ensure the necessary adaptations to its IT equipment – in order to use the link and ensure continuity of operations.

The Bank may at any time and without notice modify its own equipment, basic software and related procedures in order to optimise operations and service levels. We will provide notification of any modifications requiring adaptation of the company's equipment in order to retain the link and access by giving one month's written notice via Business Online or otherwise.

12.2. Distribution, control and storage of software

The Bank distributes the programs required to install Business Online. The company must download the programs from the Internet.

If the Bank sends CD-ROMs, they are sealed, and the company must check that the seal is unbroken. If it has been broken, the program may have been tampered with and should not be installed. The company must contact the Bank immediately for a new set.

When programs are downloaded from the Internet, the company or a user must check that the program delivery has been electronically (digitally) signed by the Bank.

If the programs have not been electronically signed by the Bank, the reason may be that they have been tampered with or do not come from the

Bank. The signature can subsequently be verified by checking the properties of the downloaded program file(s). If the electronic signature is not from the Bank, the downloaded program may not be installed.

12.3. Data security

e-Safekey and EDISec are the general security systems used in Business Online. Using both systems ensures that

- data is kept confidential (encrypted) during transmission to the Bank
- data is not modified during transmission to the Bank
- the sender is always identified
- an electronic signature is appended to all financially binding transactions

A user's electronic signature is created using a private key stored in the company's IT environment. Access to the key is protected by the user's password.

The Bank reserves the right to block the company's or user's access to Business Online if it registers attempts at misuse. If access is blocked, the company will be notified as soon as possible.

The company must implement effective security procedures to prevent unauthorised use of Business Online and unauthorised access to user keys.

13. Acquiring a user ID and a temporary PIN

When a user is to be created in Business Online, the Bank gives the user an individual user ID and a temporary PIN to be used for registering the user in the e-Safekey security system.

The temporary PIN is used for first-time identification when the user is registered in e-Safekey. The temporary PIN is

generated and printed automatically and no-one knows it. If the envelope containing the PIN has been opened or ripped, the user should contact the Bank to order a new PIN.

If the user has not received the letter with the PIN within three workdays after ordering, the user should, for safety reasons, contact the Bank to cancel it and order a new one.

When registering in the security system, the user must enter a password and subsequently destroy the temporary PIN.

13.1. Security registration and key generation

Security registration takes place before the user starts using Business Online. In this connection, a private key is generated. The key is stored in the company's IT environment and is used for generating the user's electronic (digital) signature.

Access to the key, and thus to generating electronic (digital) signatures, is protected by the password.

13.2. Password

When registering in the security system, the user must enter a password. The password protects the key against unauthorised access, thereby ensuring that electronic (digital) signatures can only be generated by the user himself or herself.

The user should select a password that is hard to guess. The password must at least be 8 characters long, and must contain both numbers, upper- and lower-case letters.

The user must ensure that others do not know the password and must store it in a suitable and safe manner, see section 13.5.

13.3. Changing the password

The company must prepare guidelines to ensure that the user regularly changes his or her password. It is the responsibility of the company to ensure that the guidelines are observed.

For further information, read the security recommendations under the Security menu item in Business Online on Fokus Bank's website and in other guidelines.

13.4. Deregistering users/keys

The company must inform the Bank if users are to be deleted. The company is responsible for all transactions performed by a user until the Bank is requested to delete or block the user.

13.5. Misuse or risk of misuse of key

The company or user must immediately contact the Bank in order to invalidate the keys if

- it is suspected that the password or the company's and/or user's key has been misused
- others have had access to the password or have gained possession of the personal key file

14. Ban on encryption

The company should be aware that local, national legislation in the country where Business Online is used may include a general ban or limitations on encryption. Therefore, national legislation should always be checked.

Part 3 – Contractual aspects

15. For business purposes only

Business Online is to be used for business purposes only. The information made available to the company, including price

information, is solely for its own use. The company may not pass on the information to others, except by written permission from the Bank.

16. Changing Business Online

Business Online gives access to the services offered by the Bank at any time.

The Bank may at any time extend the scope of Business Online without notice, whereas one month's notice is required prior to any reduction in the scope and/or content. The Bank shall provide written information of any changes via Business Online or otherwise.

17. Changes to service and support

The Bank may change the scope and content of its service and support at any time by giving one month's written notice via Business Online or otherwise. The price list shows the prices charged for the various services and support functions.

18. Responsibilities and liability

18.1. The company's responsibilities

The company uses Business Online at its own responsibility and risk.

The risk borne by the company includes, but is not limited to, the risk in relation to

- sending information to the Bank, as well as the risk that a transmission is destroyed, lost, damaged, delayed or affected by transmission errors or omissions, e.g. during intermediate handling or processing of data content
- information becoming accessible to third parties as a result of errors or unauthorised intrusion on the data transmission line
- misuse of Business Online

The company cannot hold the Bank liable for any consequences thereof.

It is the responsibility of the company to

- check that the content of User Authorisations always matches the authorisations given to the user by the company and any third party
- ensure that the content of the User Authorisation is in accordance with the company's wishes

Furthermore, it is the responsibility of the company to ensure that users are aware of the Terms and Conditions for Business Online, and that all users observe them, including that they comply with the on-screen Help.

The company is responsible for

- all operations and transactions made using the company's own key or that of a registered user
- ensuring that users keep their passwords secure so that no third party becomes aware of them
- ensuring data security in connection with storage of user keys in the company's IT environment to prevent unauthorised access to the keys
- any incorrect use or misuse of Business Online by registered users

The company cannot make any claims on the Bank in respect of errors and omissions resulting from the company's circumstances, including non-observance of safety and control procedures.

18.2. The Bank's responsibilities

The Bank will be liable for damages if, through errors or neglect, it is late in performing its obligations under the Agreement or performs its obligations inadequately.

However, the Bank is not liable for errors and omissions resulting from

- errors and omissions in third-party software which is part of the Business Online security system
- a user's disclosure of the temporary PIN and/or the password
- modifications to the security system (not performed by the Bank)
- the security system's integration with other systems or software not supplied by the Bank

In areas that are subject to stricter liability, the Bank will not be liable for losses resulting from

- IT system failure/downtime or corruption of data in these systems as a result of the events listed below, irrespective of whether the Bank operates the systems itself or has outsourced operations
- telecommunication or power failures at the Bank, statutory intervention or administrative acts, natural disasters, wars, rebellions, civil unrest, acts of sabotage, terrorism or vandalism (including computer viruses and hacking)
- strikes, lockouts, boycotts or blockades, irrespective of whether the conflict is targeted at or initiated by the Bank or its organisation and irrespective of the cause of the conflict. This also applies if the conflict affects only parts of the Bank
- any other circumstances beyond the Bank's control

The Bank's exemption from liability does not apply if

- the Bank should have predicted the circumstances resulting in the loss at the time when the agreement was concluded, or should have prevented or overcome the cause of the loss

- legislation under any circumstances renders the Bank liable for the cause of the loss

In accordance with general liability provisions in force the Bank is liable for direct losses attributable to errors made by the Bank. Apart from that, its liability is limited to remedying the deficiencies. No further claims can be made against the Bank, including for indirect or consequential damage.

19. Other terms and conditions

19.1. Structure of the Business Online Agreement

A Business Online Agreement is comprised by:

- Access Agreement Business Online
- User Authorisation(s) Business Online
- Module Description Business Online
- Terms and Conditions Business Online
- General Terms for deposits and payment orders – corporate customers
- Prices for Business Online
- The "Getting Started" user guide on the Business Online website and on-screen Help

as well as other sets of rules applying at any time, as stated in the individual Module Agreements.

By signing the Access Agreement for Business Online the Company also acknowledges having read and accepted the above set of rules, which forms part of the Agreement.

The Terms and Conditions for Business Online and other terms and conditions in force at any time are accessible at www.fokusbank.no/bedrift.

19.2. Prices

The Bank may at any time change its prices by giving written notice via Business Online or otherwise. We will debit various fees and charges from the account(s) specified as fee account(s).

19.3. Other amendments to Business Online agreements

The bank can unilaterally amend Business Online agreements, providing this is not detrimental to the company. However, the bank may also make minor amendments to conditions describing the performance of individual services or areas of use, unless the amendment will cause substantial damage or inconvenience to the company. The bank notifies the amendment in writing through Business Online or in another way.

19.4. Assignment, transfer and third parties

This Agreement has been concluded by Fokus Bank on behalf of the Danske Bank Group. This means that any member of the Danske Bank Group is entitled to fulfil and enforce this Agreement. It also means that the Bank may transfer its rights and obligations to another member of the Danske Bank Group at any time.

The Bank is entitled to transfer the performance under this Agreement to subcontractors. Such transfer shall not affect the responsibilities of the Bank under the Agreement.

20. Termination and breach

The company may terminate the Access Agreement without notice – provided that it does so in writing. Requests and agreements made before the time of termination will be carried out. Paid subscription fees will not be refunded. The Bank may terminate the Access

Agreement in writing by giving one month's notice.

The Bank may, however, terminate the Agreement without notice if the company is in breach of the Agreement, including the Terms and Conditions for Business Online. The company is in breach if it, for example, omits to pay as agreed in the Access Agreement, suspends its payments, is subject to bankruptcy proceedings or other insolvent administration of its estate, negotiates for a composition or is subject to an execution or attachment order.

21. Choice of law and legal venue

Disputes or claims and all other issues between the customer and the bank that have arisen in connection with or are linked to these business terms are to be resolved pursuant to Norwegian law, with Trondheim District Court as the legal venue.

If the company is registered for a module that is solely intended to be used abroad, the company accepts – to the same extent as the Bank – that it is subject to the legal rules and usage applying in the country where the company operates.

22. Definitions and glossary

- **Access Agreement:** Agreement between the company and Fokus Bank concerning the use of Business Online.
- **Authorisation/mandate:** Either User Authorisation for Business Online, Mandate – Corporate customers, Business Online account mandate or one of the Bank's other mandate forms for Business Online.
- **Authorisation/mandate holder:** One or more registered mandates or authorisations and/or physical persons

who have been granted authorisations/mandates.

- **Banking days:** Saturdays, Sundays, public holidays, Constitution Day and 24 December are not banking days in Norway.
- **Business Online:** Collective term used about the Bank's business systems, comprising:
 - Business PC: a PC-based payment and information system
 - Business Online: an Internet-based payment and information system
- **Confidential payments:** Confidential payments are payments (such as wages and salaries) that may only be seen or processed by users with special privileges. Payments classified as confidential can only be processed by users with these privileges.
- **Cross-border payment:** A payment is a cross-border payment if it crosses a national border – even if it involves only one transaction currency, e.g. the euro. This applies to payments between registered accounts as well as payments to unregistered accounts. In the countries where the Danske Bank Group is represented, payments between accounts in the same country are not cross-border payments.
- **Customer support:** Function at the Bank offering technical support or support for Business Online users by telephone.
- **Data delivery:** Transfer of data between customer and bank. For example, a data delivery may contain payment instructions.
- **Digital signature:** An electronic signature appended to binding transactions, e.g. payments, and used when linking to the Bank.
- **EDISec:** Security system used for other links than the programs mentioned.

- **e-Safekey:** Security system for the programs mentioned.
- **Instruction:** Electronic, written or oral request to the Bank to carry out changes, transactions, etc.
- **Keys:** Each user generates two keys (a set of keys) – a private key used to generate digital signatures and a public key used to verify the digital signature. Each user has his or her own private key in order to create unique, personal digital signatures. Access to use the keys is protected by the user's password. The keys are stored in a key file or key database on the company's IT system.
- **Master data:** First name, middle name (if any), surname, user name, customer number, national identity number and related company's address.
- **Module agreement:** An agreement containing provisions about the individual module, e.g. Trade Finance or Collection Service.
- **Module description:** Bulleted description of the functionality of the individual modules registered under the agreement.
- **On-site support:** Training, technical assistance or other assistance provided by the Bank at the company's premises.
- **Password:** A code to protect a user's private key that is used to create digital (electronic) signatures. The password has between eight and 16 characters and should include upper- and lower-case letters, as well as numbers and symbols.
- **Payments between registered accounts:** Payments between registered accounts in the same country within the Danske Bank Group
- **Security registration:** The registration process that a user must go through before using Business Online for the first time.
- **Temporary PIN:** A code issued and sent by the Bank to the company's user(s). The code consists of four or eight characters and is used by the company's user(s) to register in the Business Online/Business PC security system.
- **Transactions:** Payments, payment requests and queries in Business Online.
- **User:** A user is a person (for example an employee) who has been authorised by the company to act on its behalf via Business Online. If the company's and the Bank's IT systems are directly integrated, a user may also be a computer or system located within the company.
- **User Authorisation:** The company's authorisation of a user, specifying the services, accounts, authorisations and privileges to which the individual user has access.
- **User ID:** A six-character number assigned to the individual Business Online user. The ID might contain both numbers (digits) and upper letters. The User ID is stated in the User Authorisation.