danskebank.co.uk

# Important information

## Keeping you up to date

# Business Accounts

This booklet contains important information about changes to your agreement with us and other important information about business accounts. For your own benefit and protection, you should read it and the full Terms and Conditions carefully.

Danske Bank

## Summary of changes to your agreement with us and other important information

## BUSINESS ACCOUNTS

Dear Customer

This booklet contains important information about your agreement with us, including some changes we are making to the services we provide and useful information you should know. For your own benefit and protection, you should read this booklet carefully.

You can get a full copy of our up to date Terms and Conditions from our website at danskebank.co.uk/busdocs or by contacting us in one of the ways set out in Section 7 of this booklet and requesting a free paper copy. These are the standard Terms and Conditions we will rely on.

There are 6 matters highlighted in this booklet. These are summarised for you below, so please familiarise yourself fully with this information:

1. FRAUD – THINGS YOU NEED TO BE AWARE OF TO PROTECT YOUR PERSONAL INFORMATION AND BUSINESS BANK ACCOUNTS
   We want to make you aware of some of the methods that fraudsters use to try to access your bank account. It is important that anyone you have authorised to access your account ('an Authorised User') is also made aware of this information.
2. BUSINESS eBANKING
   We have created a guide to help you check the rights you have granted to your Authorised Users.
3. VERIFYING YOUR IDENTITY
   From 1 January 2018 we will no longer seek your consent before carrying out an electronic verification of your identity (ID).
4. VARIABLE RATE BUSINESS LOAN CUSTOMERS
   You should read this section if you have a variable rate business loan or a variable rate business investment housing loan with us and the interest reference rate that applies is Danske Bank Base Rate (UK).
5. NEW DATA PROTECTION LEGISLATION
   Impact of new Data Protection legislation on how we use and share your information.
6. TRANSACTION HISTORY
   From February 2018, when you close a business current account, we can provide you with up to 5 years of your transaction history for that account. This may be helpful for other financial matters.

Where possible we are giving you at least two months' notice of any changes to your terms and conditions. If you do not agree to these changes, you must tell us in writing before the notice period ends. In this circumstance you will have the right to end your account agreement with us before the end of the notice period. If you wish to end your agreement, you will also need to make arrangements to clear any outstanding debit balance before the end of the notice period.

You will not have to pay any extra charges if you do this. If you do not object to the changes before the end of the notice period, you will be deemed to have accepted the changes. If there is anything you do not understand, please contact your branch or Account Manager.

If any of your accounts is a joint account then, in line with the Terms and Conditions, we usually only advise the first named account holder about changes to the account Terms and Conditions. You should now ensure that any joint account holder is advised of the information referred to in this booklet. Copies of this booklet are available on our website at danskebank.co.uk/busdocs from 1 January 2018.

If you are experiencing financial difficulties, you should let us know as soon as possible. We will do all we can to help you overcome any difficulties.

We hope you find this information useful. We have provided details in Section 7 of this booklet telling you how you can contact us should you have any questions or queries.

Yours faithfully

Danny Stinton
Head of Products

# CONTENTS



If any of your accounts is a joint account then, in line with the Terms and Conditions, we usually only advise the first named account holder about changes to the account Terms and Conditions. You should now ensure that any joint account holder is advised of the changes referred to in this booklet. Copies of this booklet are available on our website at danskebank.co.uk/busdocs from 1 January 2018.

# 1. FRAUD – THINGS YOU NEED TO BE AWARE OF TO PROTECT YOUR PERSONAL INFORMATION AND BUSINESS BANK ACCOUNTS

We want to make you aware of some of the methods that fraudsters use to try to access your bank account. It is important that anyone you have authorised to access your account ('an Authorised User') is also made aware of this information.

We have set out below some of the more common types of fraud and the actions you should take to avoid them:

Our online banking system (Business eBanking) relies on all of the Business eBanking log-on details (the User ID, personal security password and the security code which is generated by the Authorised User's eSafeID device) being kept safe and known only by the Authorised User. If you want to use a Third Party Provider see the information in the next part of this Section 1. You should read the following guidance about how to keep your Business eBanking log-on details safe and secure

- Make sure that all your Authorised Users know that if they are called by a person who says that they are a bank official, or a police officer or an employee of a telecommunications or I.T. company, they should NEVER give the caller their Business eBanking passwords and if the caller asks for these details, then the caller is likely to be a fraudster
- A Danske Bank employee will NEVER contact an Authorised User by any means (phone, text or email) and ask them for all of their Business eBanking log-on details
- A Danske Bank employee or a police officer will NEVER ask an Authorised User to transfer funds to another account for "security purposes"
- If an Authorised User is in doubt about someone who says that they are calling from Danske Bank then the Authorised User should end the call and phone the Bank. The Authorised User should always phone back using a different phone or phone someone that they know and speak to them before phoning the Bank to ensure that the phone line has been cleared
- Make sure that all Authorised Users have a separate note of the Customer Support Team number and ensure that this is always the number they use: Customer Support Team 0345 850 9515*
- Ensure that all of the anti-virus and firewall protection is updated regularly on your systems and make sure that anyone using your computers does not access emails, websites or attachments which might download a virus on to your systems. We strongly recommend that all Authorised Users download Webroot SecureAnywhere® on to all PCs that are used to access Business eBanking. Webroot SecureAnywhere® is free to Business eBanking Authorised Users and is easy to download
- The safest way for Authorised Users to access Business eBanking is to type in the exact bank address in the browser (danskebank.co.uk) or from the browser favourites. Links contained in emails could take the Authorised User to a fake website that looks like ours

- If an Authorised User experiences problems logging on to Business eBanking, close the attempted session down and contact the Customer Support Team immediately on the number set out above
- You should NEVER allow remote access or share your computer screen with someone else when you log-on or are logged-on to Business eBanking
- You may also benefit from contacting your insurance broker to discuss the types of insurance that might be available to protect your business against the consequences of fraud

### If You are using the services of a Third Party Provider (TPP)

We wrote to you in November to tell you about new providers of online services known as TPPs. There are 2 types of TPP:

**Account Information Service Providers (AISPs)** – these TPPs can provide consolidated information on one or more payment accounts that you hold with more than one bank or building society. They may offer related services.

**Payment Initiation Service Providers (PISPs)** – these TPPs allow you to make online credit transfers from your bank account when you are making an online purchase. This is seen as an alternative to using a card to make these payments.

It is entirely your choice as to whether you use a TPP. A TPP cannot access your account or account information unless you give it consent to do so.

If you want to use these new services then you must be registered for Business eBanking. If the TPP uses the Open Banking Application Programming Interfaces (Open Banking APIs) then you need to tell us that you want an Authorised User (who must have a separate mandate) to be able to use these new services. Further information is set out in Section 2 of this booklet.

Depending on the technique which the TPP uses to access your account the Authorised User may need to give it his/her Business eBanking log-on details. **This is the only exception to the general rule that an Authorised User should never give anyone else these details.**

Before using a TPP you should check that it is authorised and regulated by the FCA or another European Regulator. You can do this by checking the FCA register at fca.org.uk or the European Banking Authority register at eba.europa.eu

You can find more information about TPPs on our website at danskebank.co.uk/psd2ob

### Virus attacks

Fraudsters issue bogus emails containing attachments which, if opened by the recipient, will download a virus on to the receiving computer. This means that the next time an Authorised User logs-on to Business eBanking using that computer the fraudster will be able to find out all of their Business eBanking log-on details and will be able to take over the online banking session. Meanwhile the Authorised User will not be able to log-on and may think that there is a technical fault with Business eBanking.

If you have set up your Business eBanking so that payments must be authorised

by two Authorised Users the fraudster might create a pop-up message asking for another Authorised User to input their details on the same computer or there might be a pop-up message providing the Authorised User with a phone number to call for support.

Do not be tricked by this scam. The Authorised User should immediately contact the Danske Bank Customer Support Team on 0345 850 9515*. In the meantime do not use the infected computer until a full virus check has been completed.

If you have set up your Business eBanking so that payments must be authorised by two Authorised Users you should ensure that the two Authorised Users each use different PCs when creating and then authorising payments.

### Telephone scam ('vishing')

A fraudster phones an Authorised User pretending to be a bank official and says that there is a problem with your account. Sometimes the caller seems to know where you bank and perhaps mentions the name of a bank employee to add validity to their call.

Eventually the fraudster will ask the Authorised User to either reveal all of their Business eBanking log-on details, OR they may ask the Authorised User to log-on to Business eBanking (as a virus is in place on the PC) OR ask the Authorised User to transfer funds to an account that they give.

In order to reassure the Authorised User the fraudster may ask the Authorised User to call them back immediately using the regular bank phone number. The fraudster does not hang up and so, when the Authorised User thinks he/she has phoned the bank the same line has stayed open and the Authorised User ends up talking to the fraudster again, or an accomplice.

### Email scam ('phishing') and text message scam ('smishing')

Fraudsters issue bogus emails or text messages which appear to come from the Bank asking the Authorised User to enter all of their Business eBanking log-on details. The email or text message looks authentic and provides a link to a fake log-on page. As the Authorised User enters his log-on details on the fake log-on page they will be visible to the fraudster who will use the details to log-on to Business eBanking. Meanwhile the Authorised User may get a message to say that there is a technical fault or the system may 'time out.'

If there has been a Business eBanking transaction on your account which you say that you have not authorised then you must contact us immediately to tell us. We will investigate the matter and where you are entitled to a refund we will provide you with a full refund (including any interest or charges that you incurred as a result of the unauthorised transaction) usually by the end of the next business day. When deciding whether to provide you with a refund we will take into account whether your Authorised Users have taken all reasonable steps to keep their Business eBanking log-on details safe.

### Invoice redirection fraud

This involves the fraudulent alteration of the beneficiary payment details of a genuine invoice which your business may be due to pay:

- The fraudster carries out research aiming to find out who your creditors are and what invoices are due to be paid to them and when they are due
- Sometime prior to the due payment date the fraudster will email your company (or send a letter), purporting to be a creditor, and advise you of new bank account details to which payment should be made, or
- The fraudster will email you a copy of an invoice which will bear bank account details of the fraudster's choosing
- The payment will go to the account controlled by the fraudster and will almost certainly be dispersed from there immediately by the fraudster
- The fraud will usually be discovered some time afterwards when the legitimate creditor queries non-payment of funds due to them

### Fraudulent internal email (also known as CEO Fraud)

The fraudster carries out research to find out the names of Directors and the names of those members of staff authorised to make payments on the company's behalf. The fraudster might combine this research with attempts to hack into the email accounts of key people within your business.

Eventually the fraudster will send an email, either from a hacked email account of someone within your business or from a bogus email address that appears to belong to someone within your business. The email will purport to be from the Director and instruct a person authorised to make payments, to make a payment to a bank account that is controlled by the fraudster.

Although not exhaustive, here are some examples of actions you can take to avoid being a victim of these types of fraud:

- Always authenticate requests to change fundamental elements of invoices such as bank details with the creditor. For example, make a phone call to a known contact
- Look out for different contact numbers and email addresses for creditors as these may differ from those recorded on previous correspondence
- Ensure that staff with responsibility for paying invoices look out for irregularities and changes to details on invoices and, if necessary, make contact with the creditor to verify details
- Have a set of processes and procedures which all staff adhere to in respect of authenticating internal emails which request that payments be made from your bank account

## ACTION REQUIRED

We strongly recommend that you familiarise yourself with the various security features of Business eBanking and update your settings to avail of the features you require:

- Dual authorisation of payments – with this control in place all payments need to be initiated by one Authorised User and approved by a second Authorised User before they take effect. We would also recommend that each Authorised User logs-on using a different PC
- Payment limits – using the Administration module in Business eBanking you can use payment limits to control payments executed through Business eBanking. You can create a payment limit on an account and/or on an individual Authorised User depending on your requirements
- You can implement temporary limits for periods of time determined by you, for example if your business is closed for a holiday period
- Locked creditor or beneficiary listing – using the Administration module in Business eBanking you can ensure that payments can only be made to a list of known creditors. If any new payees are added to the list then the Administrator has to separately approve this before the payment can be made

If you want to use the services of a TPP, take time to read Section 2 of this booklet and the booklet that we sent to you in November. You can get a copy of that booklet and read more about TPPs on our website at danskebank.co.uk/psd2ob

For more information on how to protect your business from fraud, visit our website danskebank.co.uk/security

*Please refer to Section 7 for information on our full contact details including opening hours

# 2. BUSINESS eBANKING

We have created a guide to help you check the rights you have granted to your Authorised Users.

- We have created a guide on our website called 'Viewing User Authorisations'. The guide provides helpful information on how you can keep track of the rights that you have granted to others to view and/or operate your accounts within Business eBanking
- If you are registered for Business eBanking, from 13 January 2018 you will be able to use the services of Third Party Providers (TPPs) to access your payment accounts

## User Authorisations

We have created a guide to help you check the authorisations that have been given to Authorised Users to view/or operate your accounts through Business eBanking. These are known as 'User Authorisations'. The guide is available on our website at danskebank.co.uk/busdocs.

It is very important that you check regularly the list of Authorised Users and the authority that has been granted to them.

If there are any changes to this list (for example if an Authorised User has left your organisation) or if you want to change the access rights of an Authorised User then you will find information on how to do this in the 'Viewing User Authorisations' guide.

Where you have granted an Authorised User access to Business eBanking we will also answer any queries regarding the accounts the Authorised User has access to when the Authorised User contacts us by telephone. We will not extend this to any other actions required, only queries.

## Using the services of a Third Party Provider to access your accounts

We wrote to you in November 2017 to explain that if you are registered for Business eBanking, from 13 January 2018 you will be able to use the services of TPPs to access your payment accounts, see details below. You might wish to review the booklet that we sent you for further information:

- If you want an Authorised User (who has a separate mandate) to be able to access your accounts through a TPP which uses the Open Banking Application Programming Interfaces (Open Banking APIs), you need to contact us and ask us to arrange this. This will only apply to access via the Open Banking APIs

- Any Authorised User who has a right to view your accounts will be able to use the services of a TPP which uses screen-scraping techniques to access your account for the purposes of Account Information Services. This means that all of the account information which is visible on the Business eBanking screens can be shared with the TPP
- Any Authorised User who can make a payment from your account using Business eBanking will be able to make a payment from your account using the services of a TPP which uses screen-scraping techniques
- Any Authorised User who has a right to make a payment from your accounts using Business eBanking will be subject to the same restrictions (for example, if two people are required to authorise a payment), whether they access the account using Business eBanking or through a TPP which uses the Open Banking APIs or a TPP which uses screen-scraping techniques
- If you have given a mandate to a third party entity to operate your accounts using Business eBanking (a Third Party Mandate), you must review that arrangement with the third party. If you want to end or change the arrangement then you must contact us
- If a third party entity has given you authority to operate their account using Business eBanking (they have given you a Third Party Mandate) then you should review the arrangement with them to make sure that they still want the arrangement to continue

We also recommend that you take time to understand the settings that each Authorised User has been granted. In this regard, we would particularly draw your attention to the additional information on Fraud which has been set out in Section 1 of this booklet.

## ACTION REQUIRED

Please take time to check the User Authorisations that apply to your accounts and make any necessary changes.

Follow the guidance on our website at danskebank.co.uk/busdocs – Business eBanking – Viewing User Authorisations.

Do carefully consider how you want your accounts to be accessed if you want to use Third Party Providers.

# 3. VERIFYING YOUR IDENTITY

From 1 January 2018 we will no longer seek your consent before carrying out an electronic verification of your identity (ID).

- We are legally obliged to carry out ID checks both when you apply for a banking service and on an ongoing basis
- From 1 January 2018, we will no longer seek your consent to carry out an electronic ID check

Under Anti-Money Laundering legislation we have a legal obligation to seek verification of your identity both when you initially apply for a banking service and on an ongoing basis.

We use the personal information that you provide to us to verify your identity, age and address, in order to prevent and detect criminal activity such as fraud and money laundering.

We use a commercial organisation to check your identity electronically. From 1 January 2018, we will no longer seek your consent before carrying out this check.

## ACTION REQUIRED

You do not need to take any action.

# 4. VARIABLE RATE BUSINESS LOAN CUSTOMERS

You should read this section if you have a variable rate business loan or a variable rate business investment housing loan with us and the interest reference rate that applies is Danske Bank Base Rate (UK).

- If we have told you that the interest reference rate on your variable rate business loan or variable rate business investment housing loan is Danske Bank Base Rate (UK) we remind you that this interest rate is set by the Bank
- If you currently have a fixed rate business loan then at the end of the fixed rate period your loan will automatically revert to a variable rate business loan with Danske Bank Base Rate (UK) as the interest reference rate
- We can change this interest reference rate at any time. The change will be effective from the beginning of the day after we announce it
- Danske Bank Base Rate (UK) is our own reference rate and is publicly available on our website and in our branches. Changes are also published in newspapers circulating in Northern Ireland

Where the interest reference rate that applies to your variable rate business loan or variable rate investment housing loan is Danske Bank Base Rate (UK) we can change that rate of interest at any time. This is our own interest reference rate and we make it publicly available.

Any change will take effect at the beginning of the day after we announce a change in the Danske Bank Base Rate (UK). If we change this rate we will publish notices on our website, in our branches and in newspapers circulating in Northern Ireland.

## ACTION REQUIRED

This is a reminder to you about how the interest reference rate on your variable rate business loan or variable rate business investment housing loan can be changed.

You do not need to take any action but if you require more information please contact your Relationship Manager or call Business Direct on 0345 850 9515*.

*Please refer to Section 7 for information on our full contact details including opening hours

# 5. NEW DATA PROTECTION LEGISLATION

Impact of new Data Protection legislation on how we use and share your information.

- You will receive clearer information in relation to how we use and store your sensitive and personal data
- You will no longer be charged for making requests to obtain your personal data

We are required to implement the new General Data Protection Regulation (GDPR) when it comes into force in May 2018. The benefit for you is that you will have greater control over your personal information and data.

The legislation places new data protection obligations on us in relation to accountability and transparency when using your information.

Under the new GDPR:

- We will be reviewing the ways in which we share your information with data processors
- When processing your information we can rely on other lawful bases apart from consent, for example where processing your information is necessary as part of our services, if we have a business need or because of legal obligations
- You will have new rights in terms of accessing your information free of charge
- You will also have the 'right to be forgotten', which means you can request the deletion or removal of personal data where there is no compelling reason for its continued processing

## ACTION REQUIRED

You will find more information on the changes to how the bank uses your personal and business information on our website at danskebank.co.uk/busdocs from 1 March 2018.

# 6. TRANSACTION HISTORY

From February 2018, when you close a business current account, we can provide you with up to 5 years of your transaction history for that account. This may be helpful for other financial matters.

- We will provide you with your transaction history when you close an account, unless you tell us you do not want to receive it
- Transaction history will cover the five year period prior to the date of closure
- The transaction history will be provided to you in an electronic 'Statement Folder' which can be accessed from danskebank.co.uk

Transaction history is the information provided in statements of account and supplementary lists. If you close the account we can provide you with up to 5 years of transaction history, free of charge, unless you opt out of receiving this information.

We will provide transaction history to you in an electronic 'Statement Folder' which is accessible on our website danskebank.co.uk – the 'Statement Folder' link will be found within the log-on button used to access Business eBanking and other digital services. We will send you a customer number and a 4 digit PIN to log-on to your 'Statement Folder'.

If you close your account and subsequently request your payment transaction history (within the 5 year period) we will provide the payment transaction history in paper format only.

## ACTION REQUIRED

You do not need to take any action.

# 7 . HOW YOU CAN CONTACT US

## You can contact us if you have any questions or wish to arrange an appointment by:

- phoning us
- writing to us through Business eBanking or by post
- through our website at danskebank.co.uk/business

## HOW TO CONTACT US BY PHONE (See Notes 1,2& 3 opposite)

| | Days | Time | Contact Number |
|---|---|---|---|
| **Corporate and Business Centre** | Monday to Friday | 8am to 8pm | 0345 2668 899<br>(+44 (0) 28 9004 9256 from outside the UK) |
| **Small Business** | Monday to Friday<br>Saturday<br>Sunday | 8am to 8 pm<br>9am to 4.30pm<br>9am to 4.30pm | 0345 8509 515 /<br>028 9004 6015<br>(+44 (0) 28 9004 6015 from outside the UK) |
| **Business eBanking customer support**<br>(technical enquiries and questions about how the service works)(see notes opposite) | | | |
| **Customer Support** | Monday to Thursday<br>Friday<br>Saturday<br>Sunday | 8am to 8pm<br>8am to 5pm<br>9am to 5pm<br>9am to 8pm | 028 9031 1377<br>(+44 (0) 28 9031 1377 from outside the UK) |
| **24 hour emergency phone numbers**<br>**Lost or Stolen cards** | | | |
| Mastercard Corporate Classic<br>From outside the UK | | | 0370 850 2489<br>+44 (0) 28 9004 9204 |
| Mastercard Corporate Platinum<br>From outside the UK | | | 0370 850 1068<br>+44 (0) 28 9004 9206 |
| Mastercard Business Debit Card<br>From outside the UK | | | 0370 850 2489<br>+44 (0) 28 9004 9204 |

## HOW TO CONTACT US IN WRITING

| Secure communication using Business eBanking or our Mobile/Tablet Business Apps. | |
|---|---|
| Our secure message function allows you to read and send messages to and from the bank: | • Log-on to Business eBanking or your App<br>• In Business eBanking select 'Contact and help' then 'Create Message' or from your App select 'Communication' then 'Create Message'<br>• Type your message and select send |

| Secure communication using our website at danskebank.co.uk/business | |
|---|---|
| To send us an email: | Go to danskebank.co.uk/email |

| By post | |
|---|---|
| Write to: | Danske Bank<br>PO Box 2111<br>Belfast<br>BT10 9EG<br>or<br>Your Account Manager |

Notes

1. Support from branches, Corporate and Business Centres, Small Business or Business eBanking customer support will not be available on Northern Ireland bank holidays or other holidays when the bank is not open for business.
2. We may record or monitor calls to confirm details of our conversations, for your protection, to train our staff and to maintain the quality of our service. Call charges may vary. Please contact your phone company for details. Customers calling from mobile phones may be charged a different rate.
3. Please note that the cost to call our Customer Services UK area codes on 0345 or 0370 within the UK is always the same as calling a local or national landline number.

Business eBanking, Danske Mobile and Tablet Business Apps may be temporarily unavailable when we are carrying out routine maintenance.

This publication is also available in Braille, in large print, on tape and on disk. Speak to a member of staff for details.

You can also read this publication on our website at danskebank.co.uk/busdocs

Danske Bank is a trading name of Northern Bank Limited and is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority. Financial Services Register reference number 122261.

Registered in Northern Ireland R568.
Registered Office:
Donegall Square West
Belfast BT1 6JS

Northern Bank Limited is a member of the Danske Bank Group.

www.danskebank.co.uk

Correct as at 01/2018

28487UK