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 agreements with us and includes details of changes we are making to the terms and conditions for some of our products and services. In each section of the booklet we tell you more about the specific changes we are making. For your own benefit and protection, you should read this booklet and the full Terms and Conditions carefully.

You can get a full copy of updated Terms and Conditions on our website at danskebank.co.uk/busdocs from 1 July 2019 or by contacting us in one of the ways set out in Section 6 of this booklet and requesting a free paper copy. These are the standard Terms and Conditions we will rely on.

There are five matters highlighted in this booklet. These are summarised for you on the contents page, so please familiarise yourself fully with these changes.

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 Relationship Manager.

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. While not included in this booklet, you can find information on the potential impacts of Brexit on the services we deliver on our website. We have provided details in Section 6 of this booklet telling you how you can contact us should you've any questions or queries.

Yours sincerely

Tim Turner
Head of Products

CONTENTS

If any of your accounts are 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 July 2019.

1. HOW TO KEEP YOUR FINANCES AND PERSONAL INFORMATION SAFE

It's important that anyone you've authorised to access your account (an 'Authorised User') is also aware of this information.

Please remember that we'll never ask you to:

- reveal PINs, the numbers from your debit or credit card, your Business eBanking logon details or passwords over the phone, through email or by text message;
- share your computer screen with us while you're logged onto Business eBanking – or ask for the numbers from your Business eBanking eSafeID security device. The codes from this device are unique to you, and no-one, not even us, should ever ask for them;
- give us remote access to your PC or mobile device;
- move money to another account for 'security purposes'. Fraudsters may claim to work for us and that funds in your account are at risk unless they're moved to a 'safe' account;
- give us any 3D Secure codes sent to your mobile when you're buying something online with a Danske card. If you receive a code when you haven't made an online purchase, please let us know.

Please remember, you should never click on any links or call a phone number received in unexpected emails or texts, or open any unexpected attachments, even if they look genuine.

Below we've set out some of the more common types of fraud and how you can avoid them:

Each Authorised user should keep their Business eBanking logon details (the UserID, personal security password and the security code generated by their eSafeID device) safe and not reveal them to anyone under any circumstances.

The only exception is when they use the services of a Third Party Provider (TPP) through Open Banking and it's authorised by the Financial Conduct Authority or another European regulator.

The following tips give you guidance on how to keep your Business eBanking logon details safe and secure.

- Make sure that all your Authorised Users know that if they're called by someone who says that they are, for example, a bank official, a police officer or an employee of a telecommunications or IT company, they should never give the caller their Business eBanking passwords. If the caller asks for these details, they're likely to be a fraudster and they should end the call immediately.
- When they're authorising payments using dual authority, each Authorised User should use a separate computer, laptop or smartphone. We won't issue a pop up message to advise you to authorise payments.
- We will never contact an Authorised User by any means (phone, text or email) and ask them for all of their Business eBanking logon 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 suspicious about someone who says that they are calling from Danske Bank, they should end the call and either phone us back using a different phone, or phone someone that they know and speak to them before phoning us again. This will make sure the phone line has been cleared.
- Make sure all Authorised Users have a separate note of the Customer Support Team number, 0345 850 9515* and ensure that this is always the number they use.
- Ensure that all antivirus 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. We provide Webroot SecureAnywhere® free to our Business eBanking Authorised Users and it is easy to download and install. Further information is available when you logon to Business eBanking.
- The safest way for Authorised Users to access Business eBanking is to type our website's address manually into their browser (danskebank.co.uk). Links in emails, even if they look genuine, could take the Authorised User to a fake website that looks like ours.
- If an Authorised User experiences problems logging on to Business eBanking, they should close the attempted session down and contact the Customer Support Team immediately.

- 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. A genuine company is very unlikely to contact you and ask you download third party software to gain remote access to your PC, tablet or mobile device.
- When you receive an email from someone you're due to pay, with their bank details, always check with that person or business that the sort code and account number they've given you are correct, by contacting them on a phone number which you know to be correct, or visiting them in person.
- You should also ask your insurance broker about insurance to protect your business against fraud.

Common types of fraud

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

Virus attacks

All Authorised Users should be suspicious of unsolicited emails which contain links, unexpected attachments or which ask them to download something. These emails may contain malware designed to compromise your device's security and in turn your Business eBanking logon details.

You can help protect your business from this type of fraud by ensuring that:

- all your Authorised Users have downloaded Webroot SecureAnywhere® to any PC used to access Business eBanking;
- payments must be authorised by two Authorised Users;
- different computers, laptops or smartphones are used to create and then authorise payments; and
- all devices used by Authorised Users to access Business eBanking have the most up-to-date system updates installed.

Some warning signs that your PC may be infected by a virus are:

- when an Authorised User enters their Business eBanking logon details a timer or waiting symbol appears;
- a pop-up may also warn the Authorised User that because of a technical problem they can't access Business eBanking;
- when an Authorised User logs on to Business eBanking a pop-up appears asking for another Authorised User to input their logon details on the same PC. This is the virus trying to find out the logon credentials of the second Authorised User so that the fraudsters can create and authorise payments.

If this happens the Authorised User should immediately contact our Customer Support Team on 0345 850 9515*. In the meantime nobody should use the infected computer until a full virus check has been completed.

Telephone call from a phone or software company

This type of scam involves a fraudster pretending to be from a software or telecommunications company, typically to tell you that your computer has a virus or a problem connecting to the internet. They'll typically ask for remote access to your PC to try and fix this. They may also tell you that you're due a refund because of inconvenience caused by this non-existent computer virus.

A genuine company is very unlikely to contact you and ask you download third party software to gain remote access to your PC.

The call may seem very convincing and may last a number of hours or consist of a number of calls, but eventually the caller will ask the Authorised User to:

- log on to their computer and carry out instructions which they give the Authoriser User;
- give them remote access to your computer while the Authorised User is logged on to Business eBanking, usually by being asked to download a piece of software such as 'TeamViewer', ' GoToMyPC' or 'LogMeIn';
- give them numbers from the eSafe ID device (either verbally or by keying them into your computer or phone); or
- provide debit or credit card details to pay for the service they're providing.

If you see a Business eBanking transaction on your account which you think you haven't authorised please contact us immediately so we can investigate.

Phishing (by email), vishing (by phone) and smishing (by text message)

These are all methods by which fraudsters can contact an Authorised User and try to trick them into revealing their Business eBanking logon details. When they first make contact they're likely to use alarmist tactics, for example telling them that there has been fraud on the account and that they need to take some action.

Fraudsters use sophisticated methods that enable them to insert a text message into a genuine text stream from us and a phishing email may also appear to be from a Danske Bank email address. Sometimes there are subtle differences in the email address for example, it may come from '@danksebank.co.uk' or '@danskebank.com.uk' instead of our genuine '@danskebank.co.uk' address. The phone number displayed on an incoming phone call may also appear to be Danske Bank's.

No matter how the fraudster has contacted the Authorised User, they will eventually ask for Business eBanking logon details either verbally or by asking

the Authorised User to enter them in an email or text message or key the details into the dialing screen of or touch tone pad of their phone. They may also ask you to download remote access software such as 'TeamViewer', 'GoToMyPC' or 'LogMeIn' in an effort to gain access to your PC.

If an Authorised User is asked to reveal all their Business eBanking logon details then it's **likely they're being targeted by a fraudster** and your business's funds are at risk.

If you see a Business eBanking transaction on your account which you don't think you authorised you must **contact us immediately** so we'll investigate the matter. Unless you're a corporate opt-out customer you have a right to an immediate refund provided that you have not acted fraudulently, with intent or with gross negligence.

We'll take into account whether you have complied with the General Terms and Conditions - Business Accounts and the Special Terms and Conditions for Business eBanking.

Payment scam

A payment scam involves you being contacted by a fraudster, usually by telephone, pretending to be someone from your bank or from the police.

They'll tell you they're investigating a serious fraud targeting the money in your bank account and that they need your cooperation in helping with their investigations.

You may even be told that a dishonest official in the bank is involved in the fraud.

Eventually, you'll be asked to transfer money from your bank account to another account, in order to supposedly keep it safe. **A police officer or a genuine member of bank staff will never ask you to do this.**

The caller will ask you not to tell anyone about this, not even your bank.

If you ever receive a call like this, **it will not be genuine!** It will be an attempt to steal your money, so you should never do what the caller tells you. You should hang up and report any such calls to the police (by calling 101), and to us.

Invoice redirection fraud

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

- The fraudster finds out who your creditors are, what invoices are due to be paid to them and when they're due.
- Before the payment date, they'll either contact your company, pretending to be one of your creditors, to tell you their bank details have changed, or they'll email you an invoice with bank account details of their choosing.
- The payment will go to the account controlled by the fraudster and will almost certainly be moved from there immediately.
- The fraud will usually be discovered some time afterwards when the legitimate creditor asks why their invoice hasn't been paid.

Fraudulent internal email (also known as CEO fraud)

The fraudster finds out the names of directors and those members of staff authorised to make payments on the company's behalf.

Eventually they'll email someone in your business with the authority to make payments, either from a hacked or bogus email address, pretending to be the director.

This email will instruct the recipient to send funds to a bank account they control. They may apply pressure to act quickly. They may also target known holiday periods, when many staff may be out of the office.

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

- Always double-check with your creditors if you get an apparent request to change something important on their invoices, such as their bank details. We recommend making a phone call to a known contact in your creditor's organisation using a known contact telephone number. Do not request confirmation of accounts details by replying to the email!
- 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 procedures for all staff on how to deal with internal emails asking for payments to be made.

ACTION REQUIRED

We strongly recommend that you familiarise yourself with the various security features of Business eBanking and update your settings to benefit from its built-in security features:

- Dual authorisation of payments – this control means all payments need to be initiated by one Authorised User and approved by a second Authorised User before they take effect. The Authorised User who authorises a payment should ensure they use a different computer, laptop or smartphone to the Authorised User who initiated the payment.
- Payment limits – using the Administration module in Business eBanking you can set a payment limit on an account, an individual Authorised User, or both.
- Temporary limits – you can set these for certain periods of time, such as when your business is closed for holidays.
- Locked creditor or beneficiary listing – you can ensure that payments can only be made to known creditors. The Administrator has to separately approve the addition of any new payees before payments can be made to them.

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

*Please refer to Section 6 for information on our full contact details including opening hours.

2. INCREASING YOUR ONLINE SECURITY

Effective from 14 September 2019

We're adding extra security steps to some of our online services.

- From 14 September 2019, you may be required to enter extra security information when you're logging on to, making payments and carrying out particular actions, on some of our channels such as 3D Secure, Corporate Expense Manager, closed account Statement Folder and Business eBanking.
- This could be another part of your Electronic Signature or an additional PIN or security code.

We're constantly reviewing the safety and security of our online channels, and we now have additional obligations under the Payment Services Regulations.

One of these is a new concept known as Strong Customer Authentication, which means you'll be required to enter extra information when you log on to some of our channels, make payments or (for example) update your email address on Business eBanking so that we can be sure it's you when you bank or make purchases online.

This information could be another part of your Electronic Signature or an additional PIN or security code.

The affected channels include:

- 3D Secure
- Corporate Expense Manager
- closed account Statement Folder, and
- Business eBanking.

ACTION REQUIRED

You don't need to do anything at the minute.
We're updating our Terms and Conditions to reflect these changes and they'll be available to view on our website by 14 September 2019. In the meantime, we'll tell you if we change any of our logon processes and send you instructions separately.

3. OPEN BANKING AND THIRD PARTY PROVIDERS (TPPs)

We've made some changes to our online services so that more Business eBanking users can allow TPPs to access your account information.

- All Business eBanking users can give a TPP permission to carry out a funds check on their account.

Some TPPs can issue cards for making payments out of your account. These TPPs can ask us to check whether you have enough funds in your account to make a particular payment. Before we respond to the TPP's first request, we'll ask you for your consent.

Any user with an Electronic Signature to access your account can give this consent. We will only respond 'yes' or 'no' to the TPPs request – we'll never provide the TPP with details of your account balance.

ACTION REQUIRED

- If you have given anyone permission to view your account, or to make payments out of it, you should check this is up to date. In particular, please remember that:
    - All Business eBanking users can use TPPs to access your account for information and funds checking services.
    - Any Business eBanking user with permission to make payments out of your account can use TPPs to initiate payments on your behalf.
- If you want to change any of your account permissions, please contact us.*
- Keep up to date with the latest developments with Open Banking at danskebank.co.uk/open-banking.

We've updated our General Terms and Conditions – Business Banking to include these changes. You can read the revised Terms and Conditions on our website at danskebank.co.uk/busdocs.

*Please refer to Section 6 for information on our full contact details including opening hours.

4. WE'RE REPLACING BUSINESS EBANKING AND INTRODUCING DIGITAL SIGNING

- We'll migrate our Business eBanking customers to District, our new online banking platform for Business and Corporate customers, throughout the second half of 2019.
- We're introducing Digital Signing for Future Financing customers.
- We've created a guide on our website called 'Viewing User Authorisations', providing helpful information on how you can keep track of the rights that you have granted to others to view and operate your accounts with Business eBanking.

Introducing District...

During 2019, we'll migrate customers from Business eBanking to District, our new online banking platform.

District will provide a modern look and feel that gives your business a better overview of your daily finances. You'll be able to access the same modules as in Business eBanking and you won't lose any functionality that you and your Users currently have.

Your current Business eBanking agreement will continue to apply when you use District and we will be in touch when you're ready to migrate to the new District platform.

...and Digital Signing

In some cases you'll now be able to sign important documents and agree to their terms by keying in your Business eBanking logon details.

This means you won't have to wait for us to post out agreements such as overdraft facility letters and Future Financing documents before you can accept their terms.

This means that:

- If you're a sole trader, you can digitally sign yourself;
- If you're a partnership, any two partners can digitally sign;
- If you're an incorporated entity (such as a limited company), you'll need to let us know which Business eBanking Users are authorised to digitally sign agreements. Please ask us for a digital signing instruction mandate to get this set up.

User Authorisations

It's very important that you regularly check the list of Users and the authorisations you've given to them to view or operate your accounts through Business eBanking.

To help you do this, we've created a guide, 'Viewing User Authorisations' which you can find at danskebank.co.uk/busdocs.

If you want to make changes to this list (for example, if a User has left your organisation or if you want to change a User's access rights) the guide will tell you how to do this.

As well as this, where you have granted a User access to Business eBanking we will also answer any queries about the accounts the User has access to when the User contacts us by telephone. We won't do any more than this – we'll just answer queries.

We also recommend that you take time to understand each User's settings, especially after reading the additional information on fraud in Section 1 of this booklet.

ACTION REQUIRED

We'll automatically migrate you to District, so you don't need to do anything.

Please check the User Authorisations that apply to your accounts and make any necessary changes by following the guidance at danskebank.co.uk/busdocs – Business eBanking – Viewing User Authorisations.

5. WE'VE INCREASED OUR FASTER PAYMENTS LIMIT

Effective Date 12 November 2018

Due to customer demand, we've increased the limit for Faster Payments in Business eBanking from £100,000 to £250,000. This new limit also applies if you want to initiate a payment using a Third Party Provider (TPP) in Open Banking.

- This change means that you can make higher value Faster Payments in Business eBanking and in Open Banking.

The Faster Payment limit in Business eBanking and Open Banking has been increased from £100,000 to £250,000 giving you more options and greater flexibility when making online payments directly or using TPPs.

ACTION REQUIRED

You don't need to do anything.

The update is reflected on our Payment Tables,

available on our website at danskebank.co.uk/busdocs.

6. 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;
- using Live Chat on our website at danskebank.co.uk/business.

HOW TO CONTACT US BY PHONE (SEE NOTES 1, 2 AND 4 OPPOSITE)

	Days	Time	Contact Number
Customer Support	Monday to Friday Saturday and Sunday	8am to 8pm 9am to 5pm	0345 8509 515 (+44 (0) 28 9004 6015 from outside the UK)
Corporate	Monday to Friday	9am to 5pm	0345 2661 166
Business Centre	Monday to Friday Saturday and Sunday	8am to 8pm 9am to 5pm	0345 2668 899 (+44 (0) 2890 049256 from outside the UK)
Business Direct	Monday to Friday Saturday Sunday	8am to 8pm 9am to 5pm 9am to 5pm	0345 2666 555 / 028 9004 9244 (+44 (0) 28 9004 9244 from outside the UK)
Business eBanking customer support (technical enquiries and questions about how the service works)(see notes below)			
Customer Support	Monday to Thursday Friday Saturday Sunday	8am to 8pm 8am to 5pm 9am to 5pm 9am to 8pm	028 9031 1377 (+44 (0) 28 9031 1377 from outside the UK)
24 hour emergency phone numbers **Lost or stolen cards**			
Mastercard Corporate Classic From outside the UK			0370 850 2489 +44 (0) 28 9004 9204
Mastercard Corporate Platinum From outside the UK			0370 850 1068 +44 (0) 28 9004 9206
Mastercard Business Debit Card From outside the UK			0370 850 2489 +44 (0) 28 9004 9204

Business eBanking Fraud	
Lost / Stolen Personal Security details / BeBanking Fraud From outside the UK	0800 917 7918 +44 (0) 800 917 7918

HOW TO CONTACT US IN WRITING

Secure communication using Business eBanking or our Mobile and Tablet Business Apps	
Business eBanking's secure email function allows you to read messages from, and send messages to, us.	• Log in to Business eBanking or the App • Select 'Contact and help' then 'Create Message' (or from your App select 'Communication' then 'Create Message') • Type your message • Send your message

Communication using our website at danskebank.co.uk/business
Chat at danskebank.co.uk/business

By post	
Write to:	Danske Bank PO Box 2111 Belfast BT10 9EG or Your Relationship Manager

Notes

1. Support from branches, Corporate and Business Centres, Business Plus or Business eBanking customer support will not be available on bank holidays or other holidays in Northern Ireland when the bank is not open for business.
2. We may record or monitor calls to confirm details of our conversations and for training and quality purposes. Call charges may vary - please contact your phone company for details.
3. Business eBanking, Danske Mobile and Tablet Business Apps may be temporarily unavailable when we are carrying out routine maintenance.
4. You can also contact our contact centre using text relay if you have any difficulty hearing.

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

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

danskebank.co.uk

Correct as at 06/2019

28490UK