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 2 January 2019 or by contacting us in one of the ways set out in Section 9 of this booklet and requesting a free paper copy. These are the standard Terms and Conditions we will rely on.

There are 8 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. We have provided details in Section 9 of this booklet telling you how you can contact us should you've any questions or queries.

Yours faithfully

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 2 January 2019.

1. HOW TO KEEP YOUR FINANCES AND PERSONAL INFORMATION SAFE

We want to make you aware of some of the methods fraudsters use to try to access your bank account or otherwise trick you into giving them money. It's important that anyone you've authorised to access your account (an 'Authorised User') is also aware of this information.

Below we've set out 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 logon details (the UserID, personal security password and the security code generated by the User's eSafeID device) being kept safe and known only by the Authorised User. An Authorised User shouldn't reveal these details to anyone.

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

The tips below 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.
- 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, to ensure the phone line has been cleared.
- Make sure all Authorised Users have a separate note of the Customer Support Team number if they need to use it, and ensure that this is always the number they use. The number is 0345 850 9515*.
- 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. 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 our website's address manually into their browser (danskebank.co.uk) or access it from their favourites. 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 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 should also ask your insurance broker about insurance to protect your business against fraud.

Virus attacks

All Authorised Users should be suspicious of unsolicited emails which contain links or which invite them to download content. These emails may contain malware designed to compromise 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; and
- different computers, laptops or smartphones are used to create and then authorise payments.

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 with Business eBanking they will be unable to access it.
- 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.

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. 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.

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. In considering this matter we will 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.

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.

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, 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 are due.
- Before the due payment date, the fraudster will either contact your company, pretending to be a creditor, and tell you their bank details have changed, or they'll email you a copy of 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.

The fraudster might attempt to hack into the email accounts of key people within your business. Eventually they will send an email, either from a hacked email account, or from a bogus email address, that appears to belong to the Director. This email will instruct a person authorised to make payments to send funds to a bank account 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 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.
- 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 to outline 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 – 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.

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

*Please refer to Section 9 for information on our full contact details including opening hours

2. WE'RE REPLACING BUSINESS eBANKING IN 2019

- We'll migrate our Business eBanking customers to District, our new online banking platform for Business and Corporate customers, throughout the first half of 2019.
- We've 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.

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.

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 www.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.

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

3. OPEN BANKING AND THIRD PARTY PROVIDERS (TPPs)

We've made some changes to make it easier for your business to access its accounts using Third Party Providers (TPPs). We'll be making more changes soon, so that different TPPs can offer Business eBanking users a wider variety of services using Open Banking.

You should read this article if you have an account with us which is accessible online. Your account, including any Danske Bank Mastercard Corporate credit card account, is accessible online unless the Special Terms and Conditions for the account state otherwise.

- Now, any Business eBanking user with a separate mandate to operate the business' accounts can use TPPs. From March 2019, users with a mandate to make payments requiring authorisation from another user will also be able to use TPPs.
- You no longer need to tell us that you want your Business eBanking users to be able to use TPPs.
- From March 2019, users will be able to make future dated payments and standing orders from the business' accounts using TPPs.
- From March 2019, users will also be able to link cards issued by a different payment service provider to the business' accounts. This means we'll be able to confirm to the provider issuing the card whether there are funds available in the account to make a payment using that card.

Open Banking is a secure way to use, compare and apply for financial products and services, giving your business control to manage, move and make the most of its money.

TPPs are authorised and regulated by the Financial Conduct Authority or another European regulator, and comply with legal and industry standards to keep your business protected.

There are two types of TPP:

- Account Information Service Providers (AISPs) – which show you a combined view of the business' accounts with different banks and building societies. They may also offer other related services.
- Payment Initiation Service Providers (PISPs) – which make online credit transfers directly from the business' bank accounts on its behalf.

Now, any Business eBanking user with a separate mandate to access and operate the business' accounts, can use TPPs. Any user who has the right to view the business' accounts can give AISPs account access but only users who have permission to make payments from the business' accounts can use PISPs.

From March 2019, Business eBanking users with a mandate to make payments that require authorisation from another user will also be able to use PISPs. Any current restrictions you've placed on

payments (for example, where another user must also authorise the payment, or there are limits on the amount of any payment that a user can make) will continue to apply to payments made through PISPs. It is important to note that payments requiring authorisation by more than one person won't be made until fully authorised. It's the responsibility of the user to inform all subsequent authorisers that a payment needs to be approved in Business eBanking. Not all PISPs may offer this enhanced functionality and where they do, users must also follow their rules to ensure that payments are made as expected. They may, for example specify a time by when the payment must be fully authorised in order for it to be made.

A TPP can only access the business' accounts where it has explicit consent to do so. This means that TPPs don't have an automatic right to information about the business, or to make payments on its behalf. For this reason, you no longer need to tell us that you want your Business eBanking users to be able to use TPPs. Each user can easily manage TPP access in Business eBanking. Simply log on, select the 'Electronic mailbox & agreements' option and click on 'Consent Dashboard' to view and cancel permissions.

At the moment, a PISP can only send single immediate payments from the business' accounts, but from March 2019, users will be able to use them to make future dated payments and payments by standing order.

From March 2019, users will also be able to link cards issued by different payment service providers to the business' accounts. This means that we'll be able to confirm to the provider issuing the card whether there are funds available in the business' accounts to make a payment using that card. We won't tell the other provider how much is in the account – we'll only reply yes or no to their request.

To find out more about this, and to keep up to date with the latest developments in Open Banking please visit our webpages at danskebank.co.uk/open-banking.

*Please refer to Section 11 for information on our full contact details including opening hours

ACTION REQUIRED

1) Check your account mandates to ensure that all user permissions for accessing and operating the business' accounts are up to date. In particular, you should bear in mind that:

- Any user with permission to view the business' accounts can use the services of a TPP for the purposes of Account Information Services.
- Any user with permission to make a payment from the business' accounts in Business eBanking can use the services of a TPP to make such payments.
- If you want to check or change any of the business' mandates then the account holder should contact us.

2) If another business has a third party mandate to operate your business' accounts using Business eBanking then you must review that arrangement. If this arrangement is to be ended or changed, then the account holder should contact us. If a different business has given your business authority to operate its accounts using Business eBanking by granting you a third party mandate then you should make sure that they still want such an arrangement to continue.

3) Users can manage TPP consents they've given in Business eBanking. You can also obtain a full list of TPPs who have access to the business' accounts by contacting us on the telephone number below.

We've updated our Terms and Conditions – Business Accounts and Special Terms and Conditions – Business eBanking and Digital Signature to take account of these changes and we've also updated the Danske Mastercard Corporate credit card terms and conditions.

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

If you have any queries about any of this, please contact us on 0345 266 6555*

*Please refer to Section 9 for information on our full contact details including opening hours

4. CURRENCY ACCOUNT TERMS AND CONDITIONS

Inter Bank Offered Rates (IBORs) will be replaced over the next few years, so we've updated our currency account terms and conditions to explain what we'll do and how it affects you.

We've also included more information about the services available on your currency account.

- The interest reference rates that we currently use are based on various IBORs – depending on the currency of the account. When an interest reference rate referred to in the terms and conditions is replaced, we'll change that interest reference rate to the replacement rate. Please be aware that we'll do this without having to ask for your consent.
- If the interest reference rate falls below zero then the interest reference rate that will apply when we're calculating interest will be zero. This means that we reserve the right, even though your account may be in credit, to charge you interest.
- We've included additional information about the payment services that are available on your currency account.

Changes to the interest reference rate

The interest rate that applies to your currency account is made up of two parts – an interest reference rate and a margin.

We use various IBORs as the interest reference rate depending on the currency of your account. When the IBOR changes we change the interest rate on your account immediately. We can also change the margin that applies. If we change the margin to your detriment we'll give you two months' notice before the change takes effect.

European Banking regulators have announced that because of concerns about how IBORs are set, they'll be replaced with alternative interest reference rates. These replacement interest reference rates will start to be used from January 2020 onwards, depending on the currency.

The replacement interest reference rates will be formally designated, nominated or recommended by the administrator of that interest reference rate or by a central bank or supervisory authority. When the replacement interest reference rates for each currency are introduced we'll replace the credit interest reference rate that applies to your account.

If you have an overdraft on your currency account, we'll contact you separately to tell you how the replacement interest reference rates will apply to your overdrawn account.

We also need to make it clear that where the interest reference rate that applies to your account falls below zero, we'll treat the rate as being zero. This means that even if your account is in credit, we reserve the right to charge you interest.

Services on your currency account

We've updated the terms and conditions to give you more information about the payment services that may be available on your currency account. By way of summary:

- We offer cheque books on Euro accounts only.
- We give you more details about the processing times that apply, for example where we send a cheque that you want to pay into your account for collection or where a SEPA Direct Debit is collected into your account.
- We give you more information about how requests for refunds of unauthorised payments, which are received after eight weeks but within 13 months of the date of the transaction, under the SEPA Direct Debit Scheme will be applied.
- Where you are registered for internet banking with us you can access your account using the services of Third Party Providers (TPPs). Later in 2019 currency accounts will be accessible by TPPs who use Open Banking. You can find more information about this at danskebank.co.uk/open-banking.

ACTION REQUIRED

You can read the updated terms and conditions at danskebank.co.uk/busdocs

5. RISKS ASSOCIATED WITH THE REFORM OF LIBOR

Proposed reforms to the London Inter Bank Offer Rate (LIBOR) may impact financial products that reference the popular benchmark.

- Financial products linked to LIBOR and maturing after 2021 may be materially impacted by the proposed reforms.

The European Union regulation on indices used as benchmarks in financial instruments and financial contracts, or to measure the performance of investment funds (the 'Benchmark Regulation'), entered into force on 1 January 2018. The Benchmark Regulation could have a material impact on products linked to a 'benchmark' rate or index. Some 'benchmarks' could also be discontinued entirely.

For example, on 27 July 2017, the Financial Conduct Authority ('FCA') announced that it will no longer persuade or compel banks to submit rates for the calculation of the LIBOR benchmark after 2021.

Should:

- the LIBOR rate not be available for any reason,
- the LIBOR rate cease to be publicly available, or
- the LIBOR rate cease accurately to reflect the rate offered by leading banks in the London Interbank market (as reported by any publicly available source of similar market data),

we will choose the applicable rate from the alternative reference rates selected by the Bank of England, FCA, Prudential Regulation Authority or any similar institution, provided always that such rate is consistent with accepted market practice.

We at Danske Bank will continue to monitor LIBOR reform developments and will provide further customer communications as the industry progresses through the LIBOR reforms.

ACTION REQUIRED

You don't have to take any action if you don't have any LIBOR linked products. If you do have LIBOR linked products maturing after 2021 it is important that you consider how the proposed LIBOR reforms may impact these products.

We're happy to support you through this process – please contact your relationship manager if you wish to discuss this matter further.

6. KEEPING YOU UP TO DATE ABOUT OUR PRODUCTS, OFFERS AND SERVICES

We'd like to keep your business up to date about our products, offers and services. It's up to you whether you want to receive this information and how you receive it.

- If you currently get updates from us, but you no longer wish to receive these, you can opt out at any time.
- Or, if you don't get updates at the minute, and you want to find out more about products, offers and services that may be of interest to your business, then you can opt in at any time.

We try to only contact you with information that we think your business might be interested in, or might benefit it.

You can change your mind about receiving this information, or how we send that information to you, at any time.

This is your right, and we'll remind you about it every two years.

If:

- you want us to stop sending you messages about our products, offers and services,
- you want us to stop sending you this information in a particular way, for example by letter, or
- you don't currently receive product, offer and service messages from us, but you'd like us to start sending these to you, then you should contact us so that we can update our records.

You can do this by:

- calling us on 0345 850 9515* (within NI/UK) or +44(0) 28 9004 6015* from outside the UK;
- completing our 'Marketing and Customer Experience Consent' form, available at any branch or from your Relationship Manager;
- writing to your branch, Relationship Manager or contact us through secure mail using Business eBanking giving your business name, address and account number and telling us what you'd like us to change about how we contact you.

ACTION REQUIRED

If you wish to change your mind about receiving product and service information then contact us in one of the ways set out above.

*Please refer to Section 9 for information on our full contact details, including opening hours.

7. INTRODUCING CONTACTLESS FOR OUR MASTERCARD DEBIT AND CREDIT CARDS

We're upgrading all new Danske Mastercard Business Debit cards (except deposit only cards) and all new Danske Mastercard Corporate cards, to include contactless technology.

You should read this article if you still have either or both:

- a Mastercard Business Debit card on your Danske Business Current Account without contactless functionality;
- a Danske Mastercard Corporate Platinum or a Danske Mastercard Corporate Classic without contactless functionality.

- Since the end of October 2018 we've been upgrading all Danske Mastercard Business Debit cards (except deposit only cards) and all new Danske Mastercard Corporate cards to include contactless technology.
- We'll upgrade your card when it's renewed or replaced, or by 30 April 2019, whichever is sooner.

We've decided to change our Mastercard Business Debit and Corporate cards so that you won't have to use your PIN to make smaller transactions.

The new cards let you:

- make contactless payments where you see the contactless symbol.
- pay with a simple tap of your card.
- stay in total control as your card never leaves your hands. You'll also have a better record of all your purchases, unlike with cash.
- pay quickly when you're in a hurry – for example at supermarkets and fast-food outlets.

For your security, each contactless transaction is limited to £30. You may occasionally be asked to provide your PIN.

There are no other changes to how you will use your account or your card.

ACTION REQUIRED

To activate the contactless function, you'll need to complete a Chip and PIN transaction first.

You should start using your new card straightaway as your existing non-contactless card will soon stop working.

You should make anyone who is a cardholder on your accounts aware of these changes.

If you are a chip and signature cardholder or a deposit cardholder, these changes won't affect you.

We've updated:

- The Special Terms and Conditions – Mastercard Business Debit; and
- the Danske Mastercard Corporate Card Terms and Conditions.

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

8. BREXIT

Effective from 29 March 2019

Depending on the outcome of the Brexit process, there could be implications for some of our customers.

- It's not yet clear what impact Brexit will have on banks and other financial services providers.
- We're considering what different Brexit scenarios could mean for you.
- If you're affected, we'll contact you once more clarity emerges from the Brexit process.

The UK is set to leave the European Union on 29 March 2019. However, there is still considerable uncertainty around what impact this will have on the financial services sector in the future.

Depending on the outcome of the Brexit process, there could be implications for some of our customers. We're continuing our work on what Brexit could mean under different scenarios and, if you're affected, we'll contact you once more clarity emerges from the Brexit process.

Once we know more about the impacts of Brexit, we'll provide details at danskebank.co.uk.

9. 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, 3 and 4 below)

	Days	Time	Contact Number
Corporate and Business Centre	Monday to Friday Saturday and Sunday	8am to 8pm 9am to 5pm	0345 266 8899 (+44 (0) 28 9004 9256 from outside the UK)
Business Direct	Monday to Friday Saturday Sunday	8am to 8pm 9am to 5pm 9am to 5pm	0345 266 6555 / 028 9004 6015 (+44 (0) 28 9004 6015 from outside the UK)
Business eBanking customer support (technical enquiries and questions about how the service works)(see notes opposite)			
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			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

Secure communication using our website 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

Correct as at 12/2018

28497UK