

Important information

Changes to Your Account Terms and Conditions

Business Customers

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

danskebank.co.uk/psd2ob

Danske **Bank**

Important Information

Changes to your agreement with us and other important information

Dear Customer

I am writing to you to tell you about changes to the Terms and Conditions for your account that will apply from 13 January 2018. These are in response to major changes in the banking industry, including new EU legislation on payment services and the introduction of Open Banking in the UK. We will explain how these changes will impact you as a customer of Danske Bank.

Open Banking is intended to make it easier for organisations to offer different and innovative services, while giving customers more choice and more control over their money and financial information.

The Payment Services Regulations 2017 (PSRs) aim to increase competition in an already competitive payments industry, bring into scope new types of payment services, enhance customer protection and security and extend the reach of the European Regulations. These European Regulations are implemented through the Payment Services Regulations 2017 in the UK.

You can read more about Open Banking and the Payment Services Regulations 2017 on our website at danskebank.co.uk/psd2ob.

How does Open Banking and the Payment Services Regulations 2017 impact my business?

This booklet contains important information about your agreement with us, including some changes we are making to the 'General Terms and Conditions - Business Accounts' and the Special Terms and Conditions that apply to the accounts and services that we provide to you. These are the standard Terms and Conditions that we will rely on from 13 January 2018 and they will apply from that date. You will find more detail about the specific changes to the Terms and Conditions within the booklet. Please read this booklet and the full Terms and Conditions carefully.

You can get a full copy of the revised Terms and Conditions on our website at danskebank.co.uk/busdocs from 13 November 2017 or by contacting us in one of the ways set out in Section 11 of this booklet and requesting a paper copy, free of charge.

The information in each section of this booklet tells you the action that you need to take.

Once you have read and understood the information, please complete the form that we have posted to you and return it to us in the prepaid envelope enclosed as soon as possible but, in any case, before 13 July 2018. If you would like to ask us about the contents of the booklet, details on how to contact us are contained in Section 11 of the booklet.

We want to highlight all of the changes that we are making to your Terms and Conditions - there are 10 topics in total, summarised for you opposite:

1. PROVIDING YOU WITH MONTHLY STATEMENTS

If we currently only make your statements available electronically in eArchive and we do not provide you with paper statements, we require your explicit consent to continue to do this. If we do not receive this authority by 13 July 2018, we will provide your statements on paper after this date.

2. THIRD PARTY PROVIDERS (TPPs)

Your Authorised Users in Business eBanking can use Third Party Providers to access your accounts. In this section we give you information about services TPPs can offer, how they provide those services and what your rights and obligations are when you use their services.

3. ELECTRONIC PAYMENTS - NON-EEA CURRENCY OR NON EEA COUNTRY

The new Payment Services Regulations introduce new rules that give you added protections when you make a payment transaction in a non-EEA currency or where only part of the transaction takes place in the EEA.

4. OUR LIABILITY TO YOU FOR PAYMENTS INTO OR OUT OF YOUR ACCOUNT

In this section, we outline our obligations to you in respect of payments into and out of your account(s).

5. MISTAKEN PAYMENTS

When a payment is made into your account by mistake, in certain circumstances we can provide your name and address to the payer to assist the payer to recover the funds. If you were the payer you may also be entitled to ask for the payee's name and address.

6. COMPLAINT HANDLING

We will respond to complaints about most payment services within 15 business days.

7. DEBIT CARDS

When you use your debit card to make a payment and you do not know the exact amount that you will be charged, you now have extra protections in relation to the amount that can be reserved.

8. HOW WE WILL CONTACT YOU SECURELY IF WE SUSPECT FRAUD ON YOUR ACCOUNT

This section tells you about the secure means we will use to contact you in the event of suspected or actual fraud or security threats.

9. OUR RIGHT TO VARY THE TERMS AND CONDITIONS OF YOUR ACCOUNT

This section tells you about the period of notice that we will give you before we change any of your Terms and Conditions and sets out the reasons that we can rely on before making such a change.

10. OUR RIGHT TO END YOUR AGREEMENT

This section tells you about the period of notice that we will give you before we end your agreement with us, including closing your account and the reasons that we can rely on before doing so.

We are giving you at least two months' notice of these 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, Account or Relationship Manager.

We hope you find this information useful. We have provided details in Section 11 of this booklet telling you how you can contact us should you have any questions or queries.

Yours faithfully



Danny Stinton

Head of Products

If you are a Corporate opt-out customer, not all of the changes in this booklet will apply to you. We have included a note to tell you where a particular change does not apply to you. These notes are at the end of the relevant sections in grey boxes, like this one.

We will be writing to you separately where you are a Corporate opt-out customer with further details.

If you are uncertain of your status, please contact us in one of the ways set out in Section 11 of this booklet.

Contents

SECTION 1	PROVIDING YOU WITH MONTHLY STATEMENTS	8
SECTION 2	THIRD PARTY PROVIDERS	9
SECTION 3	ELECTRONIC PAYMENTS - NON EEA CURRENCY OR NON EEA COUNTRY	13
SECTION 4	OUR LIABILITY TO YOU FOR PAYMENTS INTO OR OUT OF YOUR ACCOUNT	14
SECTION 5	MISTAKEN PAYMENTS	16
SECTION 6	COMPLAINT HANDLING	17
SECTION 7	DEBIT CARDS	18
SECTION 8	HOW WE WILL CONTACT YOU SECURELY IF WE SUSPECT FRAUD ON YOUR ACCOUNT	19
SECTION 9	OUR RIGHT TO VARY THE TERMS AND CONDITIONS OF YOUR ACCOUNT	20
SECTION 10	OUR RIGHT TO END YOUR AGREEMENT	21
SECTION 11	HOW YOU CAN CONTACT US	22

Glossary

In this section we explain some of the terms that we have used in this booklet.

AISP	AISP stands for Account Information Service Provider. An AISP is a Third Party Provider. An AISP provides an online service where you can see consolidated information on one or more payment accounts that you hold with more than one bank or payment service provider. An Authorised User must give authority to an AISP before it can provide this service.
Authorised User	A person you have authorised to access your account(s) using Business eBanking and to whom we have given a Digital Signature.
Authorised User with a Separate Mandate	An Authorised User who has full authority to operate your accounts using Business eBanking without the need for a second authorisation.
Chargeback rights	In certain circumstances it may be possible for us to attempt to chargeback a payment out of your account where you have used your debit or credit card to make the payment. We do this under the applicable card scheme rules. Chargeback does not give you any rights or protections and an attempt to chargeback a card transaction is not guaranteed to be successful.
Corporate opt-out	The 'Corporate opt-out' enables payment service providers to agree different terms with their customers for certain conduct of business provisions. A Corporate opt-out customer is a customer who is not a consumer, a micro-enterprise or a charity with an annual income of less than £1,000,000. In summary, a micro-enterprise is an enterprise that employs fewer than ten people and whose annual turnover and/or annual balance sheet total does not exceed €2million. Full details of the definition can be found in the Commission Recommendation 2003/361/EC
Digital Signature	This is the information that you use to log on to Business eBanking. It is made up of: <ul style="list-style-type: none">• Your User ID;• The password that you have created; and• The code from your eSafe ID device (blue fob).
EBA	EBA stands for European Banking Authority. In this booklet, we draw your attention to the fact that, from 13 January 2018, you will be able to access a list of TPPs that are authorised and regulated by a European Regulator by checking the EBA website.
EEA	EEA stands for European Economic Area, which includes countries which are in the EU and also Iceland, Liechtenstein and Norway. For the purposes of payments, Switzerland is also included. The UK is currently in the EEA.
Electronic Transfer	This is an immediate transfer of money. Sterling payments are usually made using the Faster Payments Service (FPS) and Foreign Payments are usually made using a payment system such as SWIFT.
Explicit Consent	We refer to requiring your 'explicit consent' where we have offered you a choice and we need your authority to proceed with that choice. In each instance where we have offered you a choice, we have also outlined what the position will be if you do not give us your explicit consent.
FCA	FCA stands for the Financial Conduct Authority, and is the regulator for financial services firms in the UK.

Open Banking APIs	These are the Application Programming Interfaces used by Open Banking Limited to share customer information securely. TPPs can use the Open Banking APIs.
Personalised Security Credentials	This term refers to any personalised information that you or an Authorised User uses to access your accounts, including for example: a PIN for card transactions and Digital Signature for Business eBanking.
PSD	PSD stands for the EU Payment Services Directive.
PSRs	PSRs stands for Payment Services Regulations 2017. The PSRs implement the Payment Services Directive in the UK.
PISP	PISP stands for Payment Initiation Service Provider. A PISP is a TPP which provides online services to enable a customer to initiate a payment for goods or services from an account held with the customer's bank. An Authorised User must give authority to a PISP before it can provide this service.
Screen-scraping	Screen-scraping is a technique used by some TPPs. It is a computer based programme which copies data from your computer, such as the information on your Business eBanking screens, and translates it so that the information can be displayed to you in a different way.
TPP	TPP stands for Third Party Provider. Third Party Providers are authorised and regulated by the FCA or another European Regulator.

1. Providing you with monthly statements

If you have Business eBanking then we currently make your statements available electronically in eArchive. We only send you a paper copy if you have specifically requested us to.

The Payment Services Regulations (2017) require us to provide you with a monthly statement if during any month there has been a payment transaction on your account. We will do this by sending a paper statement addressed to the account holder on our records.

If you are a Business eBanking customer then you will have the option to ask us to 'switch off' the paper statements. This means you will only receive your statements in eArchive.

What do I need to know?

- If you currently only get your statements in eArchive and you do not receive paper statements you must give us your explicit consent if you want to continue receiving your statements in this way, otherwise we will start to send you paper statements from July 2018.

WHAT DO I NEED TO DO?

- You need to tell us that you do not want us to start sending your statements on paper by completing the MY CHOICES form that we have posted to you and returning it to us in the prepaid envelope enclosed. We will continue to make your statements available electronically in eArchive.

What happens next?

- Unless you tell us that you do not want paper statements by 13 July 2018, we will start sending your statements on paper after this date. Your statements will still also be available in eArchive.
- If we currently provide you with paper statements, you do not need to take any action as this will continue however, if you are interested in getting your statements electronically you can ask us about Business eBanking.

We have changed Clause 18 in the General Terms and Conditions and the Special Terms and Conditions - Business eBanking and Digital Signature to reflect these changes.

If you are a Corporate opt-out customer these changes will not apply to you. Where you are registered for Business eBanking we will only make your statements available in eArchive and we will not start sending you paper statements.

2. Third Party Providers

From 13 January 2018 you can use the services of Third Party Providers (TPPs). TPPs are independent providers of the following types of online services:

- **Account Information Services (AIS)** – 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 also offer related services.
- **Payment Initiation Services (PIS)** – 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 and a TPP cannot access your account or account information unless you give it consent to do so.

To use the services of a TPP you must be registered for Business eBanking. A TPP can access your account using two different methods. It can use the new Open Banking APIs or it can use a technique known as ‘screen-scraping.’ Only Authorised Users will be able to use these new services. Whether your Authorised Users will be able to use a particular TPP will depend on the method which that TPP uses to access your account (see the table below)

The Open Banking APIs have only recently been developed, so some TPPs may not have developed systems to use them yet. There may also be other reasons why a TPP might use screen-scraping – for example not all payment accounts are available through the Open Banking APIs and only sterling payments can be made at this stage.

It does not matter which method is used by the TPP – it must still comply with its obligations under the Payment Services Regulations.

The two methods are compared in the table below. Words used in this table are defined in the Glossary on pages 6 and 7

	TPP that uses Open Banking APIs	TPP that uses screen-scraping
Does the TPP need to be authorised and regulated by the FCA or another European Regulator	Yes. The TPP must comply with its obligations under the PSRs.	Yes (see Note 1 on page 12). The TPP must comply with its obligations under the PSRs.

	TPP that uses Open Banking APIs	TPP that uses screen-scraping
Which Authorised Users will be able to access these services?	All Authorised Users with a Separate Mandate where you have authorised this on the MY CHOICES form.	Any of your Authorised Users. If you have placed any restrictions on the Authorised User (for example you require 2 Authorised Users to make a payment out of your account) then those same restrictions will apply when using a TPP to make a payment.
How will payment be made if the Authorised User uses a PISP?	Electronic Transfer only. You have no chargeback rights, even if there is a debit card on the account that is being accessed.	Electronic Transfer only. You have no chargeback rights, even if there is a debit card on the account that is being accessed.
What information can an AISP access?	An AISP can only access the specific information that the Authorised User authorises.	An AISP will be able to access all of the information that is visible on your Business eBanking screens.
What accounts can be accessed?	Current Accounts only. Throughout 2018 some savings accounts and corporate card accounts will also become accessible. See the list of accounts at www.danskebank.co.uk/psd2ob .	All of your accounts that are visible in Business eBanking - including current accounts, savings accounts, corporate card accounts and loan accounts.
What rights do I have - for example am I entitled to a refund if there is an unauthorised payment?	Yes - you have the same rights as you have when an Authorised User accesses your account directly.	Yes - you have the same rights as you have when an Authorised User accesses your account directly.

	TPP that uses Open Banking APIs	TPP that uses screen-scraping
How does the Authorised User provide his/her Digital Signature to authorise TPP services?	The Authorised User will be redirected by the TPP to a secure Danske Bank webpage to enter his/her Digital Signature. TPPs are obliged to have safe systems to redirect the Authorised User to the Danske Bank webpage.	The TPP may ask the Authorised User to give this information to it or it may redirect the Authorised User to the Business eBanking log on page where the Authorised user will enter his/her Digital Signature. TPPs are obliged to have safe systems for the Authorised User to provide this information.
Can an Authorised User manage access by logging into Business eBanking e.g. can an Authorised User withdraw consent that he/she has given to a TPP to access the account in the future?	Yes.	No - but the Authorised User should contact us for guidance.
What Terms and Conditions apply?	The General Terms and Conditions and the Special Terms and Conditions – Business eBanking and Digital Signature apply.	The Business eBanking and Digital Signature Terms and Conditions apply.
What do I do if I have a complaint about the TPP?	If your complaint is about a payment you should contact us. If the complaint is about a detriment you have suffered because of a data breach you should contact the AISP in the first instance.	If your complaint is about a payment you should contact us. If the complaint is about a detriment you have suffered because of a data breach you should contact the AISP in the first instance.

Note 1 – Some TPPs which were active prior to 12 January 2016 do not need to apply for authorisation until mid 2019. These TPPs cannot use the Open Banking

APIs but they can use screen-scraping. You should check the status of the TPP before using it. You can do this at fca.org.uk/firms/financial-services-register or eba.europa.eu.

WHAT DO I NEED TO DO?

1. If you want all of your Authorised Users who have a Separate Mandate to be able to access your accounts through a TPP which uses the Open Banking APIs, then you need to complete the MY CHOICES form and return it to us. This will only apply to access via the Open Banking APIs.
2. Check the mandates that you have provided to Authorised Users and make sure you do not want to change the authority that you have granted. Consider the following when carrying out your review:
 - 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 (subject to the same restrictions as apply when using Business eBanking).

If you want to change any of the mandates that you have granted then you should contact us.

3. If you have given a mandate to a different entity to operate your accounts using Business eBanking (you have given them a Third Party Mandate) then you must review that arrangement with the third party that you have authorised. If you want to end or change the arrangement then you must contact us.

If a different 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.

4. Keep a track of TPPs that have been authorised to access your account by logging on to Business eBanking. You can only do this where the TPP uses Open Banking APIs.

3. *Electronic payments - non-EEA currency or non-EEA country*

The Payment Services Regulations 2017 will increase consumer rights by extending the scope of payments that are covered in the regulations to include payments that are made in a non-EEA currency or to a non-EEA country.

What do I need to know?

- If you make an electronic payment into or out of your account in a non-EEA currency (for example US Dollars), then the part of the transaction that takes place within the EEA will have the same protections as a payment that is made in an EEA currency. These protections include, for example, the time taken to process the payment and the value dates that will apply to the payments.
- If a payment is made, in any currency, within the EEA (both the payer and payee are in the EEA), then the payee must pay any charges levied by its bank and the payer must also pay any charges levied by its bank. This is known as 'SHA'. It is the payer that must choose SHA.
- In order to make our fees clearer and more certain for you, if you are making a payment to someone who is not in the EEA and you choose 'OUR' (which means that you agree to pay both the payer's and the payee's bank charges) the current fee is £15, no matter how much the payee's bank charges.
- We have changed our Business eBanking screens and our International Money Transfer Form to make it clear to you that you must choose SHA for any payment that is made to a payee within the EEA.

In the table below, we have defined the three charging structures for making international payments.

Cost code	What does it mean if I choose this charging structure?
SHA	If you choose this, both the person sending the payment and the person receiving it pay their own bank charges for the payment. This is the standard charging structure that we will use going forward. You must use SHA if the payment is being made within the EEA.
BEN	If you choose this, the person receiving the payment pays all the bank charges for the payment.
OUR	If you choose this, the person sending the payment pays all the bank charges for the payment.

Clauses 3, 5, 6 and 7 of the General Terms and Conditions - Business have been updated to reflect the changes in the protections that apply where part of a payment transaction takes place in the EEA.

4. *Our liability to you for payments into or out of your account*

(this section does not apply to cheques or drafts)

WHAT DO I NEED TO KNOW?

When you ask us to make a payment into or out of your account we must:

- have your consent to make the payment
- process the payment in accordance with the timescales set out in the payment table
- execute the payment correctly in accordance with your instructions

You must take all reasonable steps to keep your Personalised Security Credentials (such as your Business eBanking passwords and your PIN for your debit card) safe.

If any of your Personalised Security Credentials are lost, stolen or you think that they may have been used without your authority, you must contact us immediately in one of the ways set out in the Terms and Conditions. You will not be liable for any transactions that are made from your account after you notify us.

If we fail to comply with our obligations then you may be entitled to make a claim as set out below:

1. Unauthorised transaction

If you did not give your consent in one of the ways set out in the Terms and Conditions, for a payment out of your account, we will refund the amount of the payment and any interest or charges that you had to pay as a result. We will credit your account with the amount of the refund as soon as practicable and, in any event, no later than the next business day.

Where the PSRs apply, you must make any claim within 13 months of the date that the payment was made out of your account. You must provide us with any information that we reasonably require to investigate your claim including, for example, whether you used the services of a TPP. If you did use a TPP then that will not affect your right to a refund but we need this information since we may be able to seek compensation from the TPP if it was responsible for the error.

We will not give you a refund if we are satisfied that you have acted fraudulently or with intent or gross negligence. Gross negligence would include instances where you have not taken reasonable steps to keep your Personalised Security Credentials (such as your Business eBanking password or your PIN for your debit card) safe and secure. We set out in the Terms and Conditions the steps that you must take to keep your Personalised Security Credentials safe. In certain circumstances, different rules apply where your account is overdrawn at the time that the payment is made. You can read more about this in the updated Terms and Conditions.

Payments in respect of some types of distance contracts fall outside the PSRs 2017.

For example, you are not entitled to a refund where the payment related to a distance contract for online gambling or services of a banking, credit or insurance nature. Further information is set out in the Terms and Conditions.

2. Payment transaction was executed late

We have updated the payment table to reflect the timescales within which we must process any transaction. This includes details of the cut-off times, the maximum execution times and the value dates that will apply.

If we make a payment into your account, outside these times then, except where that was due to abnormal or unforeseeable circumstances beyond our control, the consequences of which would have been unavoidable despite all our efforts to the contrary, we will restore your account to the position it would have been in had the payment not been executed late. If you make a payment out of your account and we execute it late, then if we need to, we will contact the payee's bank and ask it to put the payee's account into the position it would have been in if the payment had been executed on time.

3. Payment transaction executed incorrectly (including where you have made a mistake)

We are liable only for executing the payment in accordance with the sort code and account number (or where applicable the BIC and IBAN) for the payee that you have provided to us.

This is the case even if you have provided us with additional information such as the name of the payee or a reference number.

It is very important when giving us instructions that you check this information carefully – otherwise the payment may be paid into the wrong account and you may not be able to get it back.

We will trace a payment for you free of charge if you ask us to.

If we have not processed the payment correctly then we will restore your account to the position it would have been in had the mistake not been made or, if applicable, we will re-transmit the payment to the payee's bank.

If you have made a mistake and entered the wrong sort code and/or account number for the payee then you should ask us to use the 'Credit Payment Recovery' process to try to recover the payment. This is a banking industry process where banks work together to trace and recover mistaken payments. We tell you more about that process in the revised Terms and Conditions and also in Section 5 of this booklet.

You can read more about our liability and your liability in the revised Terms and Conditions at Clauses 6 and 7. You can also read the updated payment table.

If you are a Corporate opt-out customer these changes will not apply to you. We will write to you separately to advise you of your rights and obligations and our obligations to you under the Payment Services Regulations 2017.

5. Mistaken payments

This section tells you what will happen if you receive money into your account and the payer's bank tells us that the payer used your sort code and account number by mistake. It also explains what will happen if you make a mistake when sending a payment and accidentally use the wrong sort code and/or account number for the intended payee.

From 13 January 2018, if a payment is made into your account and the payer's bank tells us that they made a mistake and incorrectly provided your account details, then we are now obliged in certain circumstances to provide the payer's bank with your name and address details.

If you are the payer then you will have the reciprocal right in these circumstances to ask us to obtain the payee's name and address details.

What do I need to know?

- If you receive a payment that you are not expecting or that you do not recognise then you should immediately contact us and we will provide you with any information that we have that will help you to identify the payment.
- If you have received the payment by mistake, then it may be a criminal offence for you to refuse to return the payment to the payer.
- We will give you time to agree that we can return the payment to the payer. If you do not agree to do this, or there are insufficient funds in your account to do this, then we may provide your name and address details to the payer's bank and they will provide that information to their customer. They should give you further notice before they do this.
- If you are the payer and you realise that you have made a mistake, then you should contact us as soon as you become aware of the mistake and we will immediately trace the payment for you. We will contact the payee's bank and ask them to freeze the funds that were paid in error. If there are no funds in the payee's account or the payee refuses to return the funds, then we will ask the payee's bank to provide us with the name and address of the payee so that you can take further legal action to recover the funds.
- If you are the payer we cannot guarantee that you will be able to get your funds back.

WHAT DO I NEED TO DO?

- If you are making a payment out of your account, always make sure that you have used the correct sort code and account number. Be careful to ensure that you have obtained this information through a secure means. It is dangerous to use account details that have been provided to you by email. Always contact the payee directly to check this information. If you make a mistake, contact us as soon as you become aware of it.
- Check your statements carefully. If you receive a payment that you do not recognise, contact us to ask for further information about the payment. If you are not entitled to the payment then you should not spend it – you must return it to the payer.

We have changed Clause 5.5 in our General Terms and Conditions – Business Accounts and our 'How we use your personal and business information' leaflet to reflect these changes.

6. Complaint handling

The Payment Services Regulations 2017 will introduce changes to how we deal with complaints about payment services. This section tells you what is changing if you have a complaint about a payment service (other than a cheque or a sterling or foreign draft).

What do I need to know?

- If your complaint is in relation to a payment service, we will send you a final response within 15 business days or, in exceptional circumstances (for example, where we need to get information from a third party) by the end of 35 business days explaining:
 - our final response; or
 - why we cannot provide a final response yet, and when we expect to be able to do this.
- The payment services that we provide include accounts and services which permit you to make electronic payments.

- You will also be able to contact the Financial Conduct Authority (FCA) or the Payment Systems Regulator (PSR) if you think that we may have broken the Payment Services Regulations 2017.
- The FCA and the PSR will use this information to inform their regulatory activities. More information can be found at <https://www.psr.org.uk/sites/default/files/media/PDF/PSR-PSD2-approach-factsheet-Sep-2017.pdf>

These changes do not apply where your complaint is about something other than a payment service.

WHAT DO I NEED TO DO?

You should read our amended 'Putting Things Right For You' leaflet at [danskebank.co.uk/busdocs](https://www.danskebank.co.uk/busdocs).

If you are a Corporate opt-out customer you are not eligible to refer your complaint to the Financial Ombudsman Service and we do not use the services of another dispute resolution provider.

7. Debit cards

After 13 January 2018, your protection will be further enhanced when you use your debit card to make payments out of your account.

- If you use your debit card to authorise a payment out of your account and you do not know the exact amount that will be charged, then you will have further protection in relation to the amount that we can reserve on your card.

What do I need to know?

- Where you authorise a payment using your debit card and the amount of the transaction is not known in advance (for example when you hire a car or book a hotel), we will not reserve any funds on your account (reduce the available balance) unless you have authorised the exact amount that is to be reserved. We will immediately release the reservation after we have received information about the exact amount that is to be debited to your account.
- If you use a different means of payment (that is not your debit card), we may not be aware that the original reservation should be released.
- If the amount that is debited to your account is greater than you would reasonably have expected (excluding any changes that are due to exchange rate movements), then you can ask us for a refund. You must do so within 8 weeks of the date that the payment was debited. We will tell you the information that we require to consider your claim when you contact us.

WHAT DO I NEED TO DO?

You should always check your statement. If the amount debited exceeds the amount that you would reasonably have expected, then you should contact us no later than 8 weeks after the date that your account was debited and we will give you details of how to make your claim for a refund.

You should read the 'Special Terms and Conditions - Mastercard Business Debit Card', which have been updated to reflect these changes.

8. *How we will contact you securely if we suspect fraud on your account*

This section tells you about the secure means by which we will contact you if we suspect that you may have been the victim of fraud or if we suspect that you may be being targeted by fraudsters.

What do I need to know?

If we suspect that there has been fraudulent activity on your account or if we suspect that your account is being targeted by fraudsters, we will contact you by one of the secure methods noted below.

It important for you to know that, regardless of which secure means we use, we will NEVER ask you to reveal any of your Personalised Security Credentials such as any of your PIN numbers, your card numbers, or your password that you use to access and make payments on Business eBanking.

We will contact you by one or more of the following secure means:

- by phoning you using the telephone contact details we hold for you on our records. We shall identify you by asking a number of security questions; or
- by sending a letter addressed to you at the address we hold for you on our records. The letter will always quote at least the last 4 digits of your account number.

9. *Our right to vary the Terms and Conditions of your agreement*

We have changed the Terms and Conditions of your account to ensure that where we have a right to vary the Terms (such as the right to increase fees and service charges or decrease credit interest rates), we can only do this if we have a valid reason to do so. We will not vary the Terms of a Fixed Term Deposit before the end of the fixed term. These changes do not apply to any overdraft agreement that you may have with us.

What do I need to know?

1. All of our current accounts and most of our savings accounts do not have a fixed term – this means that you can continue to have the account for many years. During that time, economic and other circumstances can change and so we may need to change the Terms and Conditions that apply to your account.
2. The types of changes that we can make include changing the features and benefits of a product, changing the contractual Terms, varying the fees and service charges, introducing new fees and service charges and varying the credit interest rates that apply to the account.
3. We can only make these changes for one of the reasons that we have set out in the General Terms and Conditions. The following are examples of the reasons that we can rely on:
 - we can vary either fees and service charges or credit interest rates, to ensure that our business is profitable and competitive provided that any such change is reasonable and does not result in an account holder being treated unfairly.
 - we can increase fees and service charges where this is a proportionate response to any change in market conditions, general banking practice or the costs that we incur when providing services to our customers.
4. In future when we make a change to any of our Terms, we will tell you which reason we are relying upon to make the change. We will still give you 2 months' notice, where this is practicable, and we will always give you the right to end your agreement with us, before the change takes effect, without asking you to pay any extra charges.
5. There are some special circumstances where we can change the Terms and Conditions immediately and advise you about it afterwards. You can find more details in the General Terms and Conditions of where this applies.

WHAT DO I NEED TO DO?

Please read Clauses 16 and 26 in the revised General Terms and Conditions -Business Accounts. These will be available on our website at danskebank.co.uk/busdocs from 13 November 2017.

If you are a Corporate opt-out customer these changes will not apply to you. We will usually give you 30 days' notice before making a change to the Terms and Conditions where the change is not to your advantage. We can change the Terms and Conditions for any reason.

10. Our right to end your agreement with us

We have changed the Terms and Conditions for your account to give you clearer information about the circumstances in which we can rely upon to end your account agreement with us. We can only do this where it is fair to do so. These changes do not apply to any overdraft agreement that you may have with us.

What do I need to know?

1. We regularly review the operation of both current and savings accounts to ensure that it is still appropriate for us to provide the account. Following any such review we may decide to close your account.
2. We can only close your account for one of the reasons that we have set out in the Terms and Conditions. For example, one of the reasons we can rely on is where we have reasonable grounds to believe that you are no longer using the account.
3. It is important that you take time to read through all of the reasons that we can rely on to close your account. These are set out in Clause 20 of the General Terms and Conditions – Business Accounts.
4. We will give you 2 months' notice before we close your account. There are some special circumstances (also set out in Clause 20), such as where we reasonably suspect that your account might be used for an illegal purpose, where we can close your account immediately. In these cases we will advise you as soon as reasonably practicable that the account has been closed and the reason for our decision.

WHAT DO I NEED TO DO?

Please read Clause 20 of the revised General Terms and Conditions – Business Accounts. These can be viewed on our website at [danskebank.co.uk /busdocs](https://www.danskebank.co.uk/busdocs) from 13 November 2017.

If you are a Corporate opt-out customer these changes will not apply to you. Unless there are exceptional circumstances we will give you at least 30 days' notice before closing your account. We can close your account for any reason.

11. How you can contact us

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

- phoning us
- visiting any Danske Bank branch
- writing to us through Business eBanking or by post
- through our website at [danskebank.co.uk](https://www.danskebank.co.uk)

How to contact us by phone (See Notes 1 and 2 opposite)

	Days	Time	Contact Number
General Service	Monday to Friday Saturday and Sunday	8am to 8pm 9am to 4.30pm	0345 850 9515
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

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 in to Business eBanking or your App
- In Business eBanking select 'Contact and help' then 'Create Message' or from your App select 'Communication' then 'Create Message'
- Type your message and select send

Secure communication through our website at danskebank.co.uk/business

To send us an email:

Go to danskebank.co.uk/email

By Post

Write to:

Danske Bank
PO Box 2111
Belfast
BT10 9EG

or

Your Account Manager

or

Danske Bank
Donegall Square West
Belfast
BT1 6JS

Notes

1. Support from General Service 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, 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 UK 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.

Danske Bank is a trading name of Northern Bank Limited which is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the 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