Important information

Changes to Your Account Terms and Conditions

Personal Customers

This booklet contains important information about changes to your agreement with us and other important information about personal 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

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 on our website at danskebank.co.uk/psd2ob.

How does Open Banking and the Payment Services Regulations impact me?

This booklet contains important information about your agreement with us, including a summary of changes we are making to the 'General Terms and Conditions - Personal 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. If you are under 16 years old you should read this booklet with a parent or guardian to ensure you understand how these changes will affect you.

We have sent you a copy of the revised Terms and Conditions to your Secure Mail; you can also get these on our website at danskebank.co.uk/docs from 13 November 2017 or by contacting us in one of the ways set out in Section 10 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 10 of the booklet.

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

1. PROVIDING YOU WITH MONTHLY STATEMENTS
   If we currently make your statements available electronically in your Electronic Mailbox, we require your explicit consent to continue to do this. If we do not receive this by 13 July 2018, we will provide your statements to you on paper after this date.
2. THIRD PARTY PROVIDERS (TPPs)
   You can now 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
   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 made the payment by mistake 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 protection 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. HOW WE WILL PROVIDE YOU WITH IMPORTANT INFORMATION ABOUT CHANGES TO YOUR TERMS AND CONDITIONS
   If you would like us to send you notices of change to your Terms and Conditions electronically, we can only do that where we send you an alert.

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.

If any of your accounts is a joint account then, in line with the Terms and Conditions, we usually only advise the first named account holder about changes to the account Terms and Conditions. You should now ensure that any joint account holder is advised of the changes referred to in this booklet.

We hope you find this information useful. We have provided details in Section 10 of this booklet telling you how you can contact us should you have any questions or queries.

Yours faithfully

Danny Stinton

Head of Products

Contents

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 TPP. 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. You must give your authority to an AISP before it can provide this service.
Authorised User	A person you have authorised to access your account(s) using eBanking and to whom we have given an Electronic Signature.
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.
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 Signature	This is the information that you use to log on to eBanking. It is made up of: • Your User ID; • The passcode that you have created; and • The code from your security card.
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 this booklet, 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 use to access your accounts, for example: your PIN for card transactions and your Electronic Signature.
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. You must give your authority to a PISP before it can provide this service.
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.
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 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 are registered for our eBanking and Electronic Mailbox service, then you'll know that we currently make your statements and other transaction information available in the Electronic Mailbox section of eBanking. If you want to continue receiving these documents this way, we'll require your explicit consent.

What do I need to know?

- If we do not receive your explicit consent and we close your Electronic Mailbox then, after that date, you will receive your statements and other transaction information on paper.

WHAT DO I NEED TO DO?

- **You need to send us your explicit consent if you want to continue to receive these documents electronically. You can send us your consent by completing the form that we have posted to you and returning it to us in the prepaid envelope that we have enclosed.**

What happens next?

- If we do not receive your consent to continue to make your statements and other transaction information available in Electronic Mailbox by 13 July 2018, we will provide these documents on paper after this date and close your Electronic Mailbox on or shortly after this date.
- If we currently provide you with paper statements, you do not need to take any action as this will continue. However, if you would prefer to receive your statements and other transaction information electronically, please let us know. You must be registered for eBanking and have subscribed for Electronic Mailbox.

We have changed Clause 18 in the General Terms and Conditions and the Addendum which relates to Electronic Mailbox in the Special Terms and Conditions – eBanking to reflect these changes.

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.

To use the services of a TPP you must be registered for eBanking.

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.

If you use the services of a TPP then it 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." 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.
How will payments be made if I use a PISP?	Electronic Transfer only. You have no chargeback rights, even if there is a debit card on the account that you are accessing.	Electronic Transfer only. You have no chargeback rights, even if there is a debit card on the account that you are accessing.

2. *Third Party Providers*

	TPP that uses Open Banking APIs	TPP that uses screen-scraping
What information can an AISP access?	An AISP can only access the specific information that you authorise.	An AISP will be able to access all of the information that is visible on your eBanking screens.
What accounts can be accessed?	Current Accounts only. Throughout 2018 some savings accounts and credit 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 eBanking – including current accounts, savings accounts, credit card accounts, mortgage 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 you access your account directly.	Yes – you have the same rights as you have when you access your account directly.
How do I provide my Electronic Signature to authorise TPP services?	You will be redirected by the TPP to a secure Danske Bank webpage to enter your Electronic Signature. TPPs are obliged to have safe systems to redirect you to the Danske Bank webpage.	The TPP may ask you to give this information to it or it may redirect you to the eBanking log on page where you will enter your Electronic Signature. TPPs are obliged to have safe systems for you to provide this information.
Can I manage access by logging into my eBanking e.g. withdraw consent that I have given to a TPP to access my account in the future?	Yes.	No – but you should contact us for guidance.

	TPP that uses Open Banking APIs	TPP that uses screen-scraping
Can I tell you that I don't want to use TPP services?	If you do not want to use the services of a TPP then you can decline to use their services when you are purchasing online by choosing an alternative method of payment. If you want us to mark our records to state that you do not want to use these services then we will be able to do this from 13 January 2018 (see Note 2 on page 12).	If you do not want to use the services of a TPP then you can decline to use their services when you are purchasing online by choosing an alternative method of payment. We cannot mark our records to prevent you using these services.
Can an Authorised User on my accounts access these services?	Yes - you can tell us from 13 January 2018 if you want an Authorised User to use a TPP.	Yes.
What Terms and Conditions apply?	The General Terms and Conditions and the Special Terms and Conditions for Electronic Signature apply.	The General Terms and Conditions and the eBanking 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.

Note 2 – If your account is a joint account, then if any of the account holders asks us to block access none of the account holders will be able to access the account using the services of a TPP that uses the Open Banking APIs.

Keeping your account secure

- Before using a TPP check its status on the FCA or EBA register.
- Take all reasonable steps to keep your Electronic Signature safe.
- If you lose your Electronic Signature or you think someone else may use it without your authority – contact us immediately.
- Keep a track of TPPs that you have authorised to access your account by logging on to 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 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 – Personal 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*

(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 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 possible 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.

The Terms and Conditions set out the detailed rules that apply where you ask us for a refund. By way of summary, we will not give you a refund if we are satisfied that you have acted fraudulently or, in some cases, 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 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.

The rules are different where your account is in debit at the time that the payment is made. In these circumstances we will not give you a refund if you, or someone acting on your behalf, authorised the payment or if someone else used your your card and PIN to make the payment, having obtained them with your consent.

Where your account had a debit balance at the time the payment was made, if you make a claim later than 13 months after the payment was made it may take us longer to process a refund.

If the payment out of your account was made by Direct Debit then the terms of the Direct Debit Guarantee Scheme will apply.

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, 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 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.

If we have made a mistake, 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.

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.

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 made a mistake and used your sort code and account number by mistake. It also explains what will happen if you make a mistake when you are 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 may 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. For example, 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 5.5.11 in our General Terms and Conditions – Personal 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 that 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/docs.

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.
- Merchants can no longer apply a surcharge because you use your personal debit card to make a payment.

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 to settle the account (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.
- Merchants are no longer permitted to apply any surcharges because you use a particular card to pay for goods or services.

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 - Debit Mastercard Personal 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 in the event of suspected or actual fraud or security threats.

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 is 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 any of the numbers from your Access ID card that you use to access and make payments on 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 you an SMS (text message) to the mobile phone number that we hold for you on our records. The SMS message will ask you to contact us by phoning the number which can be obtained from the back of your card or from the Danske Bank website. The SMS will NEVER contain a link which, if selected directs you to a website or page which asks you to enter any personal or financial information such as your name, address, date of birth, PIN numbers, card numbers, numbers from your Access ID card; or
- by sending you a Secure Mail to your eBanking; 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. *How we will provide you with important information about changes to Terms & Conditions*

If we are sending you information about changes to your account Terms and Conditions electronically via Secure Mail or Electronic Mailbox in eBanking, we can only do that where we send you an alert, for example to your email address.

What do I need to know?

After 13 January 2018, we can only send important information about changes to your account Terms and Conditions to your eBanking or Electronic Mailbox if we can send you an alert. If we already have your email address, we will send an alert to your email address each time that there is an important document for you to read. We may still send you important information on paper.

WHAT DO I NEED TO DO?

Provide us with your email address or update the email address we already hold for you by completing and returning the form we have posted to you. If we are unable to send you an alert, then in future we can only send this information to you on paper.

Intentionally left blank

10. 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 eBanking or by post
- through our website at danskebank.co.uk

How to contact us by phone (See Notes 1, 2 and 3 opposite)

	Days	Time	Contact Number
General Service	Monday to Friday Saturday and Sunday	8am to 8pm 9am to 4.30pm	0345 600 2882 028 9004 9221
eBanking customer support (technical enquiries and questions about how the service works) (see the notes opposite)			
Calls within the UK	Monday to Thursday Friday Saturday and Sunday	8am-8pm* 8am-5pm* 9am to 4.30pm	0345 603 1534
Calls from outside the UK	Monday to Thursday Friday Saturday and Sunday	8am-8pm* 8am-5pm* 9am to 4.30pm	int +44 (0) 28 9004 9219

24-hour emergency phone numbers
Lost or stolen cards

Mastercard Standard, Mastercard Standard Plus & Mastercard 24/7 From outside the UK	0370 850 2481 +44 (28) 9004 9201
Mastercard Gold From outside the UK	0370 850 2482 int +44 (0) 28 9004 9202
Mastercard Platinum & Mastercard Platinum Plus From outside the UK	0370 850 2487 int +44 (0) 28 9004 9203
VISA Standard From outside the UK	0370 850 2481 int +44 (0) 28 9004 9201
Debit Mastercard From outside the UK	0370 850 2481 int +44 (0) 28 9004 9201

How to contact us in writing

Secure communication using eBanking

eBanking's Secure Mail function allows you to read and send messages to and from the bank:	• Log-on to eBanking • Select 'Contact Us' • Select 'New Message' • Type your message • Send your message

Secure communication using Danske Mobile Bank and Tablet Bank Apps

Danske Mobile Bank and Tablet Bank Apps allow you to read and send messages to and from the bank:	• Log-on to the app • Select 'Contact' or 'Contact Us and additional info" • Select 'New Message' • Type your message • Send your message

Secure communication through our website at danskebank.co.uk

To arrange an appointment:	Fill in the 'Arrange an appointment' form
Email us:	Fill in the 'Send Email to Danske Bank' form
For help with installing and using eBanking:	Fill in the 'Online Form'

By Post

Write to:	Danske Bank PO BOX 2111 Belfast BT10 9EG

Notes

1. Support from General Service or 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 refer to your phone company for more details. Customers calling from mobile phones may be charged a different rate.
3. Please note that the cost to call our Customer Services UK area codes on 0345 or 0370 within the UK is always the same as calling a local or national landline number.

* eBanking, Danske Mobile Bank and Danske Tablet Bank 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.

Correct as at 11/2017