danskebank.co.uk

Important information

Keeping you up to date

Personal Accounts

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

PERSONAL 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. If you are under 16 years old please read this booklet with a parent or guardian to ensure you understand how these changes will affect you.

You can get a full copy of the revised Terms and Conditions on our website at danskebank.co.uk/docs from 1 July 2019 or by contacting us in one of the ways set out in Section 13 of this booklet and requesting a paper copy. These are the standard Terms and Conditions we will rely on.

There are 12 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.

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

We hope you find this information useful. While not included in this booklet, you can find information on the potential impacts of Brexit on the services we deliver on our website. We have provided details in Section 13 of this booklet telling you how you can contact us should you have any questions or queries.

Yours sincerely

Tim Turner
Head of Products

CONTENTS

If any of your accounts are a joint account then, in line with the Terms and Conditions, we usually only advise the first named account holder about changes to the account Terms and Conditions. You should now ensure that any joint account holder is advised of the changes referred to in this booklet. Copies of this booklet are available on our website at danskebank.co.uk/docs from 1 July 2019.

1. HOW TO KEEP YOUR FINANCES AND PERSONAL INFORMATION SAFE

As a reminder, please remember that we'll never ask you to:

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

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

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

You should keep all of your eBanking logon details (your UserID, password (a four digit PIN) and the number from your security card, eSafeID device or Danske ID App) safe and not reveal them to anyone under any circumstances.

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

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

- If you're called by someone who says they are, for example, a bank official, a police officer or an employee of a telecommunications or IT company, you should never give them your eBanking passwords - neither by telling them the passwords directly, nor keying them into your computer screen when asked to do so nor by keying the details into the dialling screen or dialling pad of your phone. If the caller asks for these details, they're likely to be a fraudster and you should end the call immediately.

- Take care as fraudsters are able to insert their text messages into a genuine text stream from Danske Bank and the phone number displayed on an incoming phone call may also appear to be ours.
- We'll never ask you for all your eBanking logon details, by any means (phone, text or email).
- We'll never ask you to transfer funds to another account 'for security purposes'. Neither will a police officer.
- If you are in doubt about someone who tells you that they are calling from Danske Bank, you should end the call and phone us. Always phone back using a different phone or phone someone you know and speak to them before you phone us. This will make sure that the phone line has been cleared.
- Ensure that all antivirus and firewall protection is updated regularly on your computer, smartphone or tablet. We strongly recommend that you download Webroot SecureAnywhere® on to any PC that you use to access eBanking. We provide Webroot SecureAnywhere® free to our eBanking Users and it is easy to download and install. Further information is available when you logon to eBanking.
- You should never allow remote access or share your computer screen with someone else when you log on or are logged on to eBanking. A genuine company is very unlikely to contact you and ask you download third party software to gain remote access to your PC, tablet or mobile device.
- The safest way to access eBanking is to type our website's address manually into your browser (danskebank.co.uk). Links in emails, even if they look genuine, could take you to a fake website that looks like ours.
- When you receive an email from someone you're due to pay, with their bank details, always check with that person or business that the sort code and account number they've given you are correct, by contacting them on a phone number which you know to be correct, or visiting them in person.
- Be vigilant for other types of scams where fraudsters try to trick you into giving them your money.

Common types of fraud

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

Telephone call from a phone or software company

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

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

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

- log on to your computer and carry out instructions which they give you;
- give them remote access to your computer while you're logged on to eBanking, usually by being asked to download a piece of software such as 'TeamViewer', ' GoToMyPC' or 'LogMeIn';
- give them numbers from your Access ID card (that's your white security card), eSafeID device or Danske ID App either verbally or by keying them into your computer or phone; or
- provide debit or credit card details to pay for the service they're providing.

If you see a transaction on your account which you think you haven't authorised please contact us immediately so we can investigate. You have a right to an immediate refund provided that you have not acted with intent or gross negligence.

When we're deciding whether to give you a refund we'll take into account whether you have complied with the steps set out in Section 2, 3 and 4 of the Special Terms and Conditions - eBanking and Electronic Signature. If you haven't complied with these steps then we may not be able to give you a refund.

Virus attacks

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

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

- you've downloaded Webroot SecureAnywhere® to any PC used to access eBanking;
- all devices used to access eBanking have the most up-to-date system updates installed.

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

- when you enter your eBanking logon details a timer or waiting symbol appears;
- a pop-up may also warn you that because of a technical problem you can't access eBanking.

If this happens please call our Customer Support team immediately on 0800 917 7657*. 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 try to trick you into revealing your debit or credit card details or your eBanking logon details. When they first contact you they're likely to use alarmist tactics, for example telling you that there's been fraud on your account and that you need to take immediate action.

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

No matter how the fraudster has contacted you, they will eventually ask you to either reveal your debit or credit card or eBanking logon details to them either verbally or by text or by email or by keying them into the dialling screen or dialling pad of your phone. They may also ask you to download remote access software such as 'TeamViewer', 'GoToMyPC' or 'LogMeIn' in an effort to gain access to your PC.

If someone asks you to reveal all your eBanking logon details or debit or credit card details then **they're very likely to be a fraudster**. If they get the information they want from you, you're at risk of losing all available funds in your account.

Fraudulent emails requesting payment

This is when fraudsters send you an email which appears to come from someone you're due to pay money to, like a solicitor or builder. The address of the incoming email may vary slightly from the genuine email address or may come from the genuine email address which the fraudster has hacked into.

The email will either:

- ask you to send the funds to a particular bank account (identified by a 6 digit sort code and an 8 digit account number); or
- contain an amended sort code and account number to that which was previously given to you.

To avoid falling victim to this type of scam, speak directly to whoever you're due to pay. Call them using a number you know is correct or speak to them in person. Don't reply to the email to confirm their payment information.

Payment scam

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

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

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

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

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

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

Online loan and purchase scams

This involves you being contacted by someone posing as a loan company who promises to lend you money if you make a payment to them first, for example, to pay fees or taxes. If you make this payment you'll be sending money to scammers. A reputable lender will never ask you to send them money before they give you a loan.

Websites usually have recommended rules that you should follow when you're buying something, one of which is that payments for purchases should be made through the site. Be wary if the seller asks for direct payment by bank transfer.

If a seller offers you a discount to send the payment to them directly, you may be sending funds to an account controlled by a scammer (and of course you won't receive the goods either).

If you're shopping on the likes of Gumtree, Facebook Marketplace, AutoTrader or CarandClassic, be vigilant and follow the sites' advice. If you're being pressured into paying upfront to secure the sale, all may not be what it seems. You should never pay for goods before you've seen them.

Money Mule Fraud

A money mule is someone who allows their bank account to be used for illegal funds.

Often advertised as a way to make 'easy' or 'quick' money, becoming a money mule is a crime that can carry a prison sentence of up to 14 years. Your accounts will be closed and your credit score will be damaged, affecting your future ability to apply for credit like credit cards, mortgage and even phone contracts.

Money mules are often recruited through Facebook, Instagram and twitter, both by public posts or direct mails. You may also be approached in person. You'll be asked to accept a payment into your account, keep a percentage for yourself and send the rest of the money to another account.

You may also be asked to give out your debit or credit card, PIN or your eBanking logon details so a third party can access the surplus funds in your account themselves.

To avoid becoming a money mule you should:

- Be cautious of job offers which offer ‘easy’ or ‘quick’ money;
- Research any company offering these types of opportunities;
- Never allow your bank account to receive funds which do not belong to you;
- Never provide your account details (6 digit sort code and an 8 digit account number) to anyone you don’t know or trust;
- Never give your debit or credit card, PIN and/or your eBanking logon to a third party.

ACTION REQUIRED

Read the ‘Special Terms and Conditions – eBanking and Electronic Signature’ on our website at danskebank.co.uk/docs, paying particular attention to Section 2, 3 and 4 and the steps that you must take to keep your eBanking passwords and Electronic Signature safe.

If you use eBanking and at any time think that the security of your eBanking has been compromised, please call our Customer Support team* immediately and report the matter to your local police station by calling 101.

You can also read general information on how to protect yourself from online and other frauds on our website at danskebank.co.uk/keepitsafe.

Other valuable sources of information on the latest scams and frauds can be found at:

www.takefive-stopfraud.org.uk

www.nidirect.gov.uk/campaigns/scamwiseni

www.actionfraud.police.uk

www.moneymules.co.uk

www.fca.org.uk/scamsmart

*Please refer to Section 13 for information on our full contact details including opening hours.

2. REPLACING THE ACCESS ID SECURITY CARD

Effective from 14 September 2019

If you're an eBanking customer, the way you get your one-time passcodes will soon change.

- We've launched a new App, Danske ID, to generate one-time passcodes for use in eBanking. This will replace your current white plastic Access ID Security Card.
- From 14 September 2019, your Access ID Security Card will not be accepted in eBanking.

One-time passcodes from your Access ID Security Card are used across our digital banking channels as part of your Electronic Signature allowing you to log on, digitally sign documents, approve payments and send instructions to us securely.

From 14 September 2019 we're replacing these cards with Danske ID, a new App for generating one-time passcodes digitally. Danske ID, is available now from Google Play and the App Store and you'll need to download it to your smartphone to keep using eBanking after 14 September 2019.

You will need your Access ID card to install the new App and it will still be accepted in eBanking until this date so you must continue to keep it safe.

After 14 September 2019, you won't be able to use your Access ID card in eBanking and you should dispose of it safely.

If you don't have a smartphone, you can ask us for a Danske eSafe ID device. This is a fob that displays one-time passcodes for use in eBanking. Visit danskebank.co.uk/waystobank for more information.

ACTION REQUIRED

You can download our new app from the Google Play Store or the App Store now but remember to keep your current Access ID Security Card safely until 14 September as you may still need it. Please ensure you dispose of it safely after this date.

We've updated our General Terms and Conditions – Personal Accounts and Special Terms and Conditions – eBanking and Electronic Signature. These will be available at danskebank.co.uk/docs from 1 July 2019.

3. INCREASING YOUR ONLINE SECURITY

Effective from 14 September 2019

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

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

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

One of these is a new concept known as Strong Customer Authentication, which means you may be required to enter extra information when you log on to some of our channels, make payments using your debit or credit card or (for example) update your email address on eBanking so that we can be sure it's you when you bank or shop online. This extra information could be another part of your Electronic Signature, an additional PIN or security code.

The affected channels include:

- Paym
- 3D Secure
- closed account Statement Folder
- eBanking

We're also closing the Danske Text Service.

ACTION REQUIRED

You don't need to do anything at the minute.

We're updating our Terms and Conditions to reflect these changes and they'll be available to view on our website by 14 September 2019. In the meantime, we'll tell you if we change any of our logon processes and send you instructions separately.

4. INTRODUCING THE NEW DANSKE MOBILE APP

Effective from September 2019

- We launched our New Danske Mobile Bank app in April 2018, making it easier for you to manage your finances on the go.
- We'll close our current Danske Mobile Bank app (the 'Wheel') and Danske Tablet Bank in September 2019.

We launched our New Danske Mobile Bank app in April 2018. Since then, with your help, we've worked hard to develop and grow the app.

The new app allows you to:

- log on using Touch ID or Face ID;
- make external transfers up to a daily limit of £1,000 using just your passcode (no more security card);
- customise your home screen so that the app is personal to you;
- block your card if you lose it and unblock it if you find it again!

The new Danske Mobile Bank is now our primary mobile banking app. This means we'll close our Wheel app in September 2019. We'll also close Danske Tablet Bank at the same time.

Our new mobile banking app is available on iOS and Android and the good news is that you don't have to wait until September to use it – you can download it to your phone today.

ACTION REQUIRED

Download the new app today at the App Store or Google Play Store – just search for 'New Danske Bank'.

We've updated our Special Terms and Conditions – eBanking and Electronic Signature. These will be available at danskebank.co.uk/docs from 1 July 2019.

5. DANSKE CASH REWARD TERMS AND CONDITIONS

Effective from 14 September 2019

You should read this if you have a Danske Cash Reward current account.

- We're closing our Danske Tablet Bank in September 2019.
- This means that logging on to tablet banking will no longer be included in the criteria to qualify for your monthly cash reward.
- We've updated the Danske Cash Reward Special Terms and Conditions to reflect this change.

We're closing our Danske Tablet Bank in September 2019.

This change means that logging on to tablet banking will no longer be included in the criteria to qualify for your monthly cash reward.

From 14 September 2019, the criteria you must meet, on or before 6pm on the last business day of the calendar month, to qualify for your monthly cash reward will be:

- pay in at least £1,200 (not including interest, fee refunds or amounts transferred from another Danske Bank account you have); and
- log on to eBanking or mobile banking at least once (for joint accounts, at least one party to the account must do this)

ACTION REQUIRED

We've updated the Danske Cash Reward Special Terms and Conditions to reflect this change. It is important that you read carefully the updated terms and conditions. These will be available at danskebank.co.uk/docs from 1 July 2019.

6. OPEN BANKING AND THIRD PARTY PROVIDERS (TPPs)

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

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

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

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

ACTION REQUIRED

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

We've updated our General Terms and Conditions – Personal Banking to include these changes. These will be available at danskebank.co.uk/docs from 1 July 2019.

*Please refer to Section 13 for information on our full contact details including opening hours.

7. HOW WE SHOW YOUR AVAILABLE BALANCE IF YOU HAVE AN OVERDRAFT

We'll be changing how your available balance is shown on our cash machines, eBanking, and mobile apps before the end of 2019.

- Due to new regulations, we'll no longer include your arranged overdraft as part of your available balance.
- Instead, where possible we'll list your overdraft limit separately.
- This is to remind you that it's a form of debt, and separate from the money that makes up your available balance.

Your available balance is the amount of money in your account that you can spend now.

It's your account balance minus any pending debit card transactions. It doesn't always reflect every transaction - any cheques paid into your account recently that are still being processed may not show up, and contactless debits and cheques you've written might not be reflected either (so it's a good idea to keep track of those).

What's changing?

Your available balance currently includes any arranged overdraft limit you've agreed with us. When the regulations take effect this will change - your arranged overdraft limit will still be shown where possible, but separately and not as part of your available balance.

Why has this happened?

Our regulator wants to highlight the fact that if you use your overdraft, you're using a form of debt that has to be repaid, and could also lead to you being charged.

What does this mean for me?

You may see a lower available balance than you were expecting because of this change. You can still use the funds in your arranged overdraft for withdrawals and payments.

Example

Your account balance is £100, and you have an arranged overdraft of £50. You have a debit card payment of £20 waiting to be posted to your account balance.

Today your available balance will be shown as £130.

Following the change, your available balance will be shown as £80, with an arranged overdraft of £50 listed separately where possible.

ACTION REQUIRED

You don't need to do anything for now. This change will take place towards the end of this year and further details will be available on our website.

8. WHY IT'S IMPORTANT FOR US TO HAVE YOUR MOBILE NUMBERS

We use text messaging more than ever to help you manage your accounts, so it's important that we know your most up-to-date personal mobile phone number.

- Please make sure that, if you have a mobile phone, you let us know your number.
- We can text you with important information about your account, and we'll do this even more during 2019.

We'll use your mobile number to send you text alerts if, for example, you dip into an unarranged overdraft on your current account (to help you avoid charges), or if we send you an authorisation code for shopping online with your Danske card.

We'll be adding more to this service in 2019 – we'll text you if you're using your arranged overdraft which could also help you avoid charges.

ACTION REQUIRED

Do we hold your up to date mobile number? You can check or update your details through online banking, by visiting any Danske Bank branch, or by calling us.*

Mobile Bank App

- After you've logged on, tap the settings icon at the bottom right of the screen
- Tap 'Personal Information' where you can enter or update your mobile number
- You'll be asked to enter a number from your plastic security card, to save your changes.

eBanking

- After you've logged on, select 'Contact' at the top right of the screen
- Select 'Personal Data' and 'edit' - you can enter or update your mobile number and email address
- Enter your eBanking passcode and select 'OK' to save your details.

If we hold your mobile number we'll text you with further details about the new arranged overdraft alert later in the year.

*Please refer to Section 13 for information on our full contact details including opening hours.

9. REGISTERING FOR ELECTRONIC CREDIT CARD STATEMENTS

We've made some changes to our online services so that eBanking users with a Personal Danske Mastercard Credit Card can choose to have their statements delivered digitally to their electronic mailbox.

- All eBanking users can choose to have their credit card statements delivered digitally to their electronic mailbox.
- You can sign up for digital credit card statements by contacting us. We'll need your email address so that we can alert you when your statement is available to view.
- You can change back to getting paper statements at any time.

If you're an eBanking user you may already get account statements and other transactional information sent to your Electronic Mailbox. Now, you can also choose to get your credit card statements in this way.

Switching to digital credit card statements is easy – simply contact us and we'll make the change for you. We'll need your email address so that we can alert you each time your statement is ready to view.

This way, you can be sure that you don't miss important information, such as your payment date. We'll also start sending you alerts telling you when your other account statements are available but you can turn these off if you don't want to receive them.

Don't worry if you find that digital credit card statements aren't working for you – just tell us and we'll switch you back to getting paper statements.

ACTION REQUIRED

If you would like to start receiving digital credit card statements, contact us and have your email address close to hand.

We've updated our General Terms and Conditions – Personal Banking, our Special Terms and Conditions – eBanking and Electronic Signature and our Personal Danske Mastercard Credit Card Terms and Conditions to include these changes. These will be available at danskebank.co.uk/docs from 1 July 2019.

10. DEADLINE APPROACHING FOR PAYMENT PROTECTION INSURANCE (PPI) COMPLAINTS

Deadline Approaching for Payment Protection Insurance (PPI) Complaints.

The Financial Conduct Authority has set 29 August 2019 as the deadline for customers to make a complaint if they feel they were mis-sold Payment Protection Insurance (PPI).

You might have had PPI if you've taken out or used loan or credit products with us, such as:

- loan – this includes personal loans and business loans
- credit card
- mortgages

You need to refer your complaint to us or to the Financial Ombudsman Service on or before the 29 August 2019 deadline (by 11.59pm) or you may lose your right to have your complaint assessed. You shouldn't wait until 29 August 2019 - act sooner rather than later to check if you had PPI and decide whether to complain.

If you had PPI you can complain yourself – for free – and claim back money you've paid for the policy or policies. By complaining yourself, you can avoid paying a claims management company.

If you want to make a PPI complaint, and haven't already done so, please phone or call into your local branch.

ACTION REQUIRED

Please contact us as soon as possible, as, complaints received after the deadline date of 29 August 2019 may not be considered.

11. IF YOU HAVE A VARIABLE RATE MORTGAGE OR PERSONAL LOAN WITH US

Please read this article if you have a mortgage or personal loan with us, and you're paying a variable rate of interest.

This article tells you:

- how Danske Bank Base Rate (UK), our interest reference rate, can change;
- that we have a right to vary the Danske Bank Standard Variable Rate (UK) and the Danske Bank Re:pay Rate (UK); and
- how to contact us if you're paying Standard Variable Rate on your mortgage and you'd like to ask about other options.

What happens if we change Danske Bank Base Rate (UK)

We'd like to remind you that, if the interest rate you're paying on your loan is calculated with reference to Danske Bank Base Rate (UK), it can change at any time. This is our own interest reference rate and it's publicly available on our website and in our branches.

We'll advertise any change in the Danske Bank Base Rate (UK) on our website, in our branches and in newspapers published in Northern Ireland.

It will take effect at the beginning of the day after we announce it. We'll also keep you informed about any interest rate changes in the periodic statements we send you.

Our right to vary Danske Bank Standard Variable Rate (UK) and Danske Bank Re:pay Rate (UK)

If the rate of interest you're paying on your mortgage or personal loan is a variable rate published by us (for example, the Danske Bank Standard Variable Rate (UK)), we may vary this at any time. This might be for any of the reasons set out in the General Offer Conditions we've previously given you.

If we're going to do this, we'll advertise this on our website, in our branches and in newspapers published in Northern Ireland. Any change will take immediate effect on the date we specify in the adverts.

We may also vary the interest rate for any other valid reason, as long as we do this in a way that's proportionate and reasonable.

Do you have a Standard Variable Rate mortgage?

If your mortgage reverted from an introductory offer to our Standard Variable Rate, you may benefit from repackaging to another Danske mortgage.

Have a look at danskebank.co.uk/mortgages to see what else we could offer you.

ACTION REQUIRED

You don't need to do anything, but if you'd like to speak to us.*

*Please refer to Section 13 for information on our full contact details including opening hours.

12. IF YOU HAVE A DANSKE CASH ISA OR JUNIOR CASH ISA WITH US

Effective from 14 September 2019

Please read this article if you have a Danske Cash ISA or Junior Cash ISA (JISA) account with us.

- We're changing the notice we'll give you if we reduce the interest rate on your account.
- You'll no longer be able to access your account online using Third Party Providers (TPPs) in Open Banking.

From 14 September 2019, we'll now tell you about any reduction in the credit interest rate payable on your ISA or JISA at least 14 days' before the new rate is applied to your account. If we decide to do this, you'll be able to cancel your agreement before the end of this 14 day notice period, if you wish.

If we decide to increase the credit interest rate payable on your account, we'll continue to apply this change immediately.

We've also made some changes to the ways in which you can access your accounts online. Whilst you can continue to view and make payments from or to your ISA and to your JISA using eBanking, you can no longer use TPP services, as these accounts are not payment accounts under the Payment Services Regulations 2017.

ACTION REQUIRED

We've updated the Danske Cash ISA and Junior Cash ISA Special Terms and Conditions to reflect these changes. These will be available at danskebank.co.uk/docs from 1 July 2019.

13. 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 eBanking or by post;
- using live chat on our website at danskebank.co.uk.

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

	Days	Time	Contact Number
General Service	Monday to Friday Saturday and Sunday	8am to 8pm 9am to 5pm	028 9004 9221/ 0345 600 2882
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 to 8pm 8am to 5pm 9am to 4.30pm	0345 603 1534
Calls from outside the UK	Monday to Thursday Friday Saturday and Sunday	8am to 10pm 8am to 5pm 9am to 4.30pm	+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 (0) 28 9004 9201
Mastercard Gold From outside the UK			0370 850 2482 +44 (0) 28 9004 9202
Mastercard Platinum & Mastercard Platinum Plus From outside the UK			0370 850 2487 +44 (0) 28 9004 9203
Debit Mastercard From outside the UK			0370 850 2481 +44 (0) 28 9004 9201
eBanking Fraud			
Lost / Stolen Personal Security details / eBanking Fraud From outside the UK			0800 917 7657 +44 (0) 800 917 7657

HOW TO CONTACT US IN WRITING

Secure communication using eBanking or our Mobile Bank App	
eBanking's secure email function allows you to read messages from, and send messages to, us.	• Log on to eBanking or the App • Select 'Contact' (or from the App tap 'Messages' and then the pencil icon to type your message).
Chat via eBanking	• Log on to eBanking • Select Chat

Communication using our website at danskebank.co.uk	
Chat:	Go to danskebank.co.uk/enquiry
For help with installing and using eBanking:	Go to danskebank.co.uk/ebankingsetup

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, and for training and quality purposes. Call charges may vary - please refer to your phone company for details.
3. eBanking, Danske Mobile Bank and Danske Tablet Bank 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/docs

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

danskebank.co.uk

Correct as at 06/2019

28491UK