# Online Banking Terms and Conditions and Privacy Policy

TESCO Bank

These terms and conditions are our agreement with you for Online Banking and our Mobile Banking App – they tell you how our Online Banking and our Mobile Banking App work.

You'll need to read them along with the terms and conditions for each of your Tesco Bank products, which tell you how you make payments, and what happens if anything goes wrong, for example if there's a payment that you didn't authorise.

Full details of how we use your information are set out in the product terms and conditions, but there's some extra information in the Privacy Notice at the end of these terms and conditions.

# Accessing Online Banking and the Mobile Banking App

## What security details do I need to access Online Banking and the Mobile Banking App?

To log in to Online Banking and the Mobile Banking App, we'll ask you to enter:

- Your Username.
- Two digits from your Security Number.
- Your full password.
- On the Mobile Banking App, you can also set up a five-digit passcode to use instead of your other security details.
- Some devices may also allow you to log in or authorise transactions using a fingerprint or face.

## Can I access Online Banking or the Mobile Banking App from any device?

When you log in we'll check if you're using a device you've asked us to recognise. Each time you successfully log in from a device we don't recognise, we'll ask if you want us to remember it in the future. You can ask us to recognise as many devices as you like, but you shouldn't ask us to recognise public computers – they might not be secure.

## What if you don't recognise my device?

If you log in and you're not using a device you've asked us to recognise, we'll use some additional security to make sure it's really you logging in. We'll send you a One Time Access Code by text message, which you must use to log in.

By sending this code to the mobile number you've given us, we can be confident it's really you logging in, so it's really important that you keep us up to date if you change your number. If you don't have a mobile phone you can only log in to Online Banking from the device you used when you registered.

## What if I reset or change my Tesco Bank security details?

If you ever need to reset or change your password, then for security reasons, we'll forget any devices that you've previously asked us to recognise. This means each time you log in from one of those devices after you've changed your password, we'll send you a One Time Access Code.

## What systems do I need to access Online Banking?

We support the latest versions of:

- Internet Explorer
- Chrome
- Firefox
- Safari

If you're using one of these, you shouldn't have any problems accessing Online Banking, although if you're using an older version sometimes you may find some features don't work quite as you expected.

Browsers are always being updated, so the most up to date versions may not be entirely compatible.

## Can I access the Mobile Banking App from any device?

The Mobile Banking App is only available on Apple and Android devices. We don't currently support any other mobile platforms.

You'll need to have registered for Online Banking before you can use the Mobile Banking App. You must only register the Mobile Banking App on your own phone. Do not use anyone else's phone to access the app.

You should only download the Mobile Banking App from the App Store or Google Play – it's the only way that you can be sure you're downloading the right app and we won't be liable if you download from anywhere else.

It's best not to root or "jailbreak" your phone – it makes it less secure, and we can't guarantee that the Mobile Banking App will work, or that your data will be secure. Our systems can detect some methods of rooting or jailbreaking. To protect your security, we may prevent you from using the Mobile Banking App.

## What do I need to use the Mobile Banking App?

To access the Mobile Banking App on your device we recommend you use the most recent version of iOS or Android. We'll tell you which versions are supported when you download the app from the App Store or Google Play. We may stop supporting versions at any time.

If your device doesn't meet these minimum requirements you may not be able to access the Mobile Banking App, or some features may not work as expected.

# Protecting your accounts

## What should I do to keep my accounts secure?

**You must:**

- Keep all Tesco Bank security details secret (this includes your login details for Online Banking and the Mobile Banking App
  e.g. your Username, Security Number, Password and Passcode) and take reasonable precautions to prevent them becoming known to another person, other than authorised third party providers (see below). If your device stores a fingerprint or face, you should not store anyone else's fingerprint or face on your device. You will be liable for all transactions which are authorised using any fingerprint or face that is stored or added to your device.
- Take reasonable steps to maintain the security of your device, for example:
  - Make sure your device is locked when you're not using it.
  - Keep your device free of viruses, malware or spyware.
  - Log out of Online Banking or the Mobile Banking App when you've finished (you should never rely on us automatically logging you out).
  - Avoid using unsecure or unencrypted Wi-Fi.
  - Only use public Wi-Fi hotspots if you know they are trustworthy – fraudsters can set up malicious Wi-Fi networks that could intercept your data.

**You must not:**

- Write down or record your Tesco Bank security details in a way which could be understood by someone else.
- Take a screenshot or screen capture of your security details as they are being entered.
- Other than an authorised third party provider, let anyone else know or use your Tesco Bank security details (not even a joint account holder – they'll have their own).
- Leave your device unattended after you've logged in to Online Banking or your Mobile Banking App.
- Let anyone else use your device if you are logged in to Online Banking or your Mobile Banking App.
- Set up a public computer as a computer you want us to recognise e.g. in an internet cafe.
- Register the Mobile Banking App on someone else's device.

## Using Authorised Third Party Provider (TPP) Services

To use these services, you will need to allow the TPP access to your online banking by sharing your security credentials.

To keep your accounts secure when using a TPP:

- Only use providers authorised by the FCA, or another European regulator.
- Remember that once you have shared your details with an authorised TPP, they will be able to see all of your accounts that appear on online banking.
- Be aware that once a TPP has access to your account information, Tesco Bank will have no control over how this data is used.

To stop using a TPP services and to prevent them from continuing to access your account(s) you must first contact the TPP to withdraw your consent to use their services, and then should update your security details with us to prevent further access to your accounts.

Please refer to your product terms and conditions for more information.

## What if I think someone knows my Tesco Bank Online Banking or Mobile Banking App security details?

- You must contact us immediately and change your Tesco Bank security details straight away.

## What if I forget or lock my Tesco Bank security details?

If you've forgotten your existing details or you are locked out of Online Banking or the Mobile Banking App, you can reset them online. We may need to send you a Temporary Security Number by text message or post to make sure it's really you.

## What should I do if my phone is stolen?

Call our Online Helpdesk immediately so that we can block the Tesco Bank Mobile App being accessed on your stolen phone. If you suspect that someone else knows any of your log in details then ask us to reset them when you call.

## What if I want to change my Tesco Bank security details?

If you want to change your security details, you can do so by logging in to Online Banking and choosing Manage Security Details on the Online Banking Overview or by contacting us.

## What if I'm asked for my Tesco Bank Online Banking security details?

Once you've registered, we'll never ask for all of your security details when we contact you.

If you ever receive a request for all of your details at any time (by email or otherwise), don't give them out and report it to us straightaway by emailing phishing@tescobank.com. You'll never be asked for your security details or your PIN by online retailers, so you should never disclose them, even to the police or other security agency.

# When you might not be able to use Online Banking or the Mobile Banking App

## Are there times when I can't access or make transactions with Online Banking or the Mobile Banking App?

For your or our protection we can block your access to Online Banking and the Mobile Banking App. We'll only do this if we reasonably think it's necessary because:

- We believe your Tesco Bank security details may have been compromised.
- We believe that the security of your device has been compromised, for example if it has been rooted or jailbroken.
- We're informed of a dispute between you and a joint party with whom you operate the account, or the death of you or a joint party to the account. You should check the terms and conditions for your product for the specific circumstances.
- There's suspected fraudulent or unauthorised use of the Tesco Bank security details.
- Your accounts have been closed.

We can stop you using Online Banking and the Mobile Banking App if we reasonably believe that the security of our systems is at risk or we think that you have broken either these terms and conditions or the terms and conditions governing your account(s) in a serious way. If we do this we will try to give you notice but in some situations we may stop the services straight away.

You should check your product terms and conditions for specific circumstances when we may block access to your account or refuse a transaction for these (or other) reasons.

## What about system maintenance?

There may be times, planned or unplanned, when Online Banking or the Mobile Banking App are unavailable. If they're not available, you can always contact us and we'll do what we can to help.

## I'm going abroad – can I use Online Banking or the Mobile Banking App?

There might be some countries where some or all of Online Banking or the Mobile Banking App doesn't work. If you need to access your account, please contact us by phone.

Remember your mobile phone network provider may charge you if you use mobile data to access our Online Banking or Mobile Banking services when abroad and data roaming charges can be expensive.

## Can I manage an account with a power of attorney using Online Banking or the Mobile Banking App?

If you manage an account with a power of attorney, you can only do this using telephone banking.

# Anything else I need to know about using the Mobile Banking App?

## How does ATM Finder work?

To use this service you must activate 'location services' functionality in your phone/device so we can detect your location to find the nearest ATM.

## How do I find out about updates to the Mobile Banking App?

Sometimes we'll ask you to update the Mobile Banking App – you'll either need to go to the App Store/Google Play to install updates or they might update automatically if you have that functionality turned on.

We're constantly updating the Mobile Banking App (adding new features and improving existing features), so after an update, we might not support older versions of iOS/Android.

## The Mobile Banking App is software – do I need a licence to use it?

The content of the app (which includes future updates) is protected by copyright, trademarks, database and other intellectual property rights. This means when you download the app we automatically give you the right (a licence) to use and display the content of the app on your device for personal use but you can't:

- Transfer or sub-license the licence to anybody else.
- Copy or reproduce any part of the app.
- Alter the app in any way.
- Try to obtain any of our source code (the IT which makes this work).

If there is a claim by a third party that the Mobile Banking App infringes their intellectual property rights, Tesco Bank will be solely responsible for dealing with any such claim.

The licence starts when you download the Mobile Banking App and will remain in place until you uninstall the app or if you fail to comply with the terms set out above.

# Changes to these terms and conditions

We can change any part of these terms and conditions. We will always act reasonably when we do so. These terms and conditions will only be changed for any of the following reasons:

- We reasonably believe that the change would make the terms easier to understand or fairer to you.
- We need to make the change as a result of changes in law, the decision of an Ombudsman or any other regulatory requirement (or where we reasonably expect that there will be a change of this type. If the expected change is not made we'll change the terms and conditions back).
- We're making changes as a result of changes in industry codes or agreements, technology or the systems we use to run our business, or to reflect good banking practice but we'll only do this if it is as favourable or more favourable to you.
- To introduce new services.

If we make a change for any of these reasons we will tell you about the change at least 30 days before the change by letting you know in Online Banking or in-App messaging that they're changing. Where the changes are to your advantage, or if it's not possible to tell you 30 days in advance, we'll tell you as soon as we can.

We can also change the terms for any reason not set out in these terms and conditions. You are free to stop using the Online Banking and the Mobile Banking App at any time if you do not want to accept any change we make.

Sometimes we might make changes to the way that Online Banking or the Mobile Banking App operates and will ask you to read and accept new terms and conditions before you continue. This is for your own safety and security, so you will not be able to continue unless you accept them.

# Our liability to you

We will not be liable if we break this agreement due (directly or indirectly) to:

(a) Abnormal and unforeseen circumstances outside our control the consequences of which would have been unavoidable despite our best efforts – this may include the failure of any machine, data processing system or transmission link or delays and failures due to industrial action.

(b) Our obligations under UK or European Union law.

We will not be liable to you:

(a) For any loss of business, loss of goodwill, loss of opportunity or loss of profit in any circumstances.

(b) For any loss to you we could not have reasonably anticipated when you gave us the instruction.

Nothing in this agreement will stop us being liable if we act fraudulently, with gross negligence or we are at fault and the law does not permit us to limit or exclude liability.

If we choose not to enforce any terms and conditions under this agreement, we will be able to apply them again at any time.

# Other information

If your address is in Scotland, Scots law applies to the contract between us and disputes between us will be referred to the Scottish courts. If your address is elsewhere, English law will apply and disputes will be referred to the English and Welsh courts.

We will communicate with you in English and you can ask for a copy of this document at any time.

We may transfer our rights and duties under our agreement with you to another company in the future (this is sometimes called an assignation). We will only do this if we reasonably believe they will treat you to the same standard as we have. Tesco Bank is a trading name of Tesco Personal Finance plc, registered in Scotland No. SC173199. Registered Office:
2 South Gyle Crescent, Edinburgh EH12 9FQ

We are authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Our registration number is 186022. You can check this on the FCA's Register by visiting **www.fca.org.uk/firms/systems-reporting/register** or by contacting the FCA on **0800 111 6768** or PRA on **0207 601 4878**.

# How to make a complaint

If you wish to make a complaint you can do so by contacting us at:

**Savings:** 0345 678 5678*

Tesco Bank Savings Operations, PO Box 27017, Glasgow G2 9FH

**Loans:** 0345 600 6016*

Tesco Bank Loan Operations, PO Box 27014, Glasgow G2 9FE

**Credit Cards:** 0345 300 4278*

Tesco Bank Credit Card Operations, PO Box 27028, Glasgow G2 9FT

**Current Accounts:** 0345 835 3353*

Tesco Bank Current Account Operations, PO Box 17430, Edinburgh EH12 1HZ

If you make a complaint, we'll aim to resolve it as quickly as we can. If you're not happy with our response to your complaint, you may be able to refer your complaint to the Financial Ombudsman Service (FOS).

You can find out more about the FOS by writing to them at Exchange Tower, London E14 9SR or by telephoning on **08000 234 567**. Details are also available from their website: **www.financial-ombudsman.org.uk**

*This number may be included as part of any inclusive call minutes provided by your phone operator.

# Privacy policy

## About your information and Data Protection

The details below tell you how we will use the information you provide to us by using our Tesco Bank Online Banking (which includes our Mobile Banking App). This should be read with the **'About your information and Data Protection'** section of your product terms and conditions which gives you more details.

By using the Online Banking or our Mobile Banking App you are giving your consent to us using your information in the ways described below and the ways explained in your product terms and conditions.

Tesco Personal Finance plc, trading as Tesco Bank, is the Data Controller and is part of the Tesco Group.

## What sort of information do you hold about me and how do you collect it?

The information that we may collect and store will include any information you enter and submit on this website, including your name, address, email addresses and any banking details or transactions.

We might also collect your IP address and other unique information to identify the device you are accessing Online Banking from. This will be used for analysis purposes to help us understand how you use our website and the Mobile Banking App and to help us improve our service. We might also collect information from your device and Wi-Fi connection to assist us in making sure the Mobile Banking App is safe to use on your device and in detecting and preventing fraud (such as mobile number, IMEI number, application and device logs including malware presence, root or jailbreak status and location). It will not be used to personally identify you, unless we suspect fraud.

- If you use the ATM Finder service you will need to enable location services. By enabling location services you allow us to collect information which is then used in our assessments of whether a transaction is unusual and may be fraudulent. This is done for your security. We also collect some location information for analysis purposes, to help us improve our service. If you do not wish us to collect and use your geolocation data in this way, you should turn off location services for the Mobile Banking App on your device.
- If you choose not to allow the Mobile Banking App to access location services we won't capture your location data. You'll be able to use the Mobile Banking App as normal apart from the ATM finder. You can control access to location services at any time through your phone settings.

## What do you do with my information?

Your information will be used to process and provide any service that you request of us. The security information you set up will be used to help prevent unauthorised or fraudulent use of your Online Banking or Mobile Banking App.

We may use your contact details (mobile phone or postal address) when we set up or register your security details to confirm your identity. We may transfer and store your information outside the European Economic Area, but we will ensure that appropriate security measures are taken.

## Cookies and security tokens

If you use our Online Banking or Mobile Banking App, we'll use a small file (security token) which is similar to a cookie to identify your device you've asked us to recognise. This is a method of identifying trusted devices and we'll never use the security token to track your usage on the internet. The security token will only be used when you login to Online Banking or use the Mobile Banking App.

Cookies are small text files placed on your device and are commonly used on the internet. We use two types of cookie:

Session cookies – these are temporary and are deleted as soon as you close your browser.

Persistent cookies – these are stored on your device until they expire or you remove them. We do not use cookies to track your use of the internet after you've left Online Banking or our Mobile Banking App, nor do we store any personal information in them that others could read and understand. More information about cookies can be found in the Privacy & Cookies section of our website.