

Getting started on Bankline: administrator's guide

This guide explains what happens next, and what you need to do to start using Bankline as an administrator

Your role as an administrator

Administrator Duties

As an administrator, you will be responsible for most of the support functions for your users. This includes:

User Management

- Create, edit, suspend and delete users
- Re-activate a user who has been disabled after entering their PIN or password incorrectly
- Order a new activation code when a user has forgotten their password
- Specify how often users must change their password
- Manage roles - Control accounts and functions to which users have access

Account Control

- Set up dual administration and dual authorisation
- Choose which of your accounts users can access in Bankline
- Add or remove accounts from view
- Mark accounts as confidential so only authorised users can access them
- Set and make changes to payment limits

We suggest that you have more than one administrator set up to look after these activities. If you are using dual administration, set up no less than three administrators.

What happens now?

To get started you will need to have received the following items; to learn more about these and how and when you will receive them please see the descriptions below. **When you have received everything, you will need to log into Bankline no later than 21 days after your Customer ID and User ID email was received.**

Getting Started Checklist



Email containing your Customer ID and User ID

This will arrive the same day as your welcome email. Your company will have the same Customer ID for all users but User IDs are specific to each user of Bankline. You will use this to log into Bankline going forward.



User Smartcard

This will arrive within **7-10 working days** and will be sent to your main address for the attention of the user that you first gave when signing up to Bankline.

This should only be used by the user whose name is on the card. Smartcards are used to authorise certain changes and payments on Bankline.



Letter containing your Smartcard PIN

This will arrive within **7-10 working days** and will be sent to the card users address on Bankline addressed to them. It is 4-6 digits and to reveal the PIN simply peel off the panel and place the panel on top of a white background. The PIN is on the panel not the letter. Smartcard PINs are unique to each card; you will have to change the PIN before you start using Bankline.



Bankline Smartcard Reader

This will arrive within **7-10 working days** and will be sent to your main address for the attention of the user that you first gave when signing up to Bankline.

Your card readers are universal and can be used by any of your Bankline users. Once you are set up on Bankline it is worth while ordering a spare card reader so you always have one to hand. Instructions on how to do this can be found in section 4.3.



Letter containing your Activation Code

This will arrive within **7-10 working days** and will be sent to the user's address on Bankline, addressed to them. It is 10 digits and to reveal the code peel off the panel at the back of the letter and scratch the surface to reveal a grey panel. Place this panel onto a white background to see the code. You will only need to use this code once to set up Bankline.

Next Steps

Now that you have received all of the items on the 'Getting Started Checklist' you will need to activate your Bankline Smartcard.

1. First you will need to change the PIN for your Smartcard

To do this:

You will need your Smartcard, Smartcard Reader and Smartcard PIN letter (pin on the back of the peeled off panel)

Put your Smartcard firmly into the Smartcard Reader, chip first and facing upwards

1. Press the 'ON/OFF' button, the Smartcard Reader will now ask you to enter your PIN
2. Enter the 4-6 digit PIN on the letter with the card holders name on it and press green 'OK' button
3. Provided that the PIN has been entered correctly, the reader will now prompt you to enter a 'NEW PIN' that you want to use going forward, this should be memorable, different from the PIN supplied and 4 digits long

Tip: You are also required to set up a PIN for logging into Bankline as well as your Smartcard PIN and these can be the same if required: To do this your PIN cannot be ascending or descending order or contain more than two consecutive numbers

4. Re-enter the new PIN once the 'REPEAT PIN' message has appeared on the display
5. Then select the green 'OK' button to confirm
6. On acceptance of the new PIN, the reader will display 'PIN CHANGED' or 'press sign or info' this means that your card is now active

If it reads 'ERROR' or 'NEW PIN NOT ACCEPTED' please try the process again

1.1 Authorising Changes with Your Smartcard and Reader

Your card is used to authorise certain changes and payments on Bankline, you may need to authorise changes during set up.

Using a Smartcard Reader to authorise changes:

1. Click Administration on the left hand side, select Smartcard Authorisation
2. Tick the box next to role to be authorised and click Authorise Selected
3. You will be prompted to perform Token Authorisation to complete the action, this means using your Smartcard Reader

When prompted, Bankline will display a Challenge code. Here is how you use it in your Smartcard Reader:

4. Put the Smartcard in the Smartcard Reader and turn Smartcard Reader on
5. Press 'SIGN' and enter the challenge code from Bankline
6. Press 'OK'
7. Enter your PIN and press 'OK'
8. The Smartcard Reader will generate a display 10-digit password, which you enter onto Bankline in the space it provides
9. Click Go
10. Click Continue



If you have dual administration another administrator must log on to Bankline and follow the steps below:

11. Click Administration
12. Click Authorise Change
13. Click changes underlined in the Details field
14. Click Accept Changes
15. If prompted with a challenge code, repeat steps 4-10



Alternatively there is a video on the Bankline Support Centre on 'Authorising changes with your Smartcard'

2. Logging into Bankline for the First Time

Once you have activated your Smartcard you can now log into the Bankline website for the first time.

Always log into Bankline by typing in the full web address www.rbs.co.uk/bankline do not save this as a link or a favourite. We recommend doing this to ensure you are always on the most up to date version of Bankline and avoid fraudulent sites.

To Log into Bankline:

You will need your Bankline Customer ID and User ID email and 10 digit activation code letter (code on the grey panel)

1. Go to www.rbs.co.uk/bankline and click Log in at the top right hand corner
2. Enter the Customer ID and User ID you received by email and then enter your Activation Code. This is a 10 digit number
3. Now you need to create your own PIN and password

PIN must be: 4 digits long with no more than two consecutive numbers. Numbers cannot be in an ascending / descending sequence

Password must be: 6-20 alphanumeric characters. (It will not be case sensitive)

You will need to change this every 28 days but you can amend this frequency once logged into Bankline

4. Click Confirm

Please destroy your Activation Code. From here on in, we will ask you for your Customer ID and User ID and random characters from your PIN and password

When you first log in, you will be able to view account information but won't have access to payments.

This is because although you are an 'Administrator' you need to assign the 'privileges' that you require on Bankline (only Administrators can set up and manage roles).

At this point you are now ready to make payments on Bankline

Please visit the Bankline Support Centre for future support when using Bankline, where you can view PDFs, videos and sign up for training calls with our experienced advisors.

<http://www.rbs.co.uk/bankline>

Billing

We will calculate our charge for our online service each month. We will tell you what we are charging for the previous month, by sending you a notification through Bankline on day 1 of each month. We will apply the charge to your account on day 15 of each month, or the next working day.

You can see your Bankline charges online:

- Click View Notification to see a detailed breakdown.

Please refer any billing queries to your Relationship or Business Manager

Please see section 8 of the Bankline Terms & Conditions for more information and section 9 for termination information.

Where to get Help

Help is available online within the Bankline service through our FAQs or for an extensive range of guides please visit the Bankline Support Centre at: <http://www.rbs.co.uk/bankline>

You may also call the Bankline Support Team, our contact details can be found on the bottom of the Bankline Support Centre Pages.

Important security information

Organised criminals are consistently developing ever-more sophisticated tactics to target UK and Irish businesses. Vishing and Phishing attacks (the use of telephone and email by fraudsters to obtain information required to perpetrate fraud) are increasing across the banking industry and fraudsters have been successful in obtaining customer log in and payment authorisation information from customers.

Failing to secure your PCs and/or failing to keep Bankline PINs, passwords and Smartcard codes secure, may leave your business liable for any losses in the event that a fraudulent incident occurs.

HOW CAN YOU PROTECT YOUR BUSINESS FROM CURRENT THREATS?

Never release your online banking or payment authorisation details over the phone or by email – to any 3rd party.

Ensure your staff are aware of the following key points in relation to their Bankline credentials:

We will **never** ask for your full PIN & password online: only 3 random digits from each are needed to log in

We will **never** ask for your PIN & password or any Smartcard codes over the telephone: beware of imposters

We will **never** ask for Smartcard codes to log in: these codes are used to authorise payments

Never open attachments from unknown sources – doing so could infect your PC

We recommend you download Trusteer Rapport free security software from www.rbs.co.uk/Rapportsecurity

This document has been prepared by The Royal Bank of Scotland plc or an affiliated entity ("RBS") exclusively for internal consideration by the recipient (the "Recipient" or "you") for information purposes only. This document is incomplete without reference to, and should be viewed solely in conjunction with, any oral briefing provided by RBS. RBS and its affiliates, connected companies, employees or clients may have an interest in financial instruments of the type described in this document and/or in related financial instruments. Such interests may include dealing in, trading, holding or acting as market-maker in such instruments and may include providing banking, credit and other financial services to any company or issuer of securities or financial instruments referred to herein. RBS is not and shall not be obliged to update or correct any information contained in this document. This document is provided for discussion purposes only and its content should not be treated as advice of any kind. This document does not constitute an offer or invitation to enter into any engagement or transaction or an offer or invitation for the sale, purchase, exchange or transfer of any securities or a recommendation to enter into any transaction, and is not intended to form the basis of any investment decision. This material does not take into account the particular investment objectives, financial conditions, or needs of individual clients. RBS will not act and has not acted as your legal, tax, regulatory, accounting or investment adviser; nor does RBS owe any fiduciary duties to you in connection with this, and/or any related transaction and no reliance may be placed on RBS for investment advice or recommendations of any sort. Neither this document nor our analyses are, nor purport to be, appraisals or valuations of the assets, securities or business(es) of the Recipient or any transaction counterparty. RBS makes no representation, warranty, undertaking or assurance of any kind (express or implied) with respect to the adequacy, accuracy, completeness or reasonableness of this document, and disclaims all liability for any use you, your affiliates, connected companies, employees, or your advisers make of it. Any views expressed in this document (including statements or forecasts) constitute the judgment of RBS as of the date given and are subject to change without notice. RBS does not undertake to update this document or determine the accuracy or reasonableness of information or assumptions contained herein. RBS accepts no liability whatsoever for any direct, indirect or consequential losses (in contract, tort or otherwise) arising from the use of this material or reliance on the information contained herein. However, this shall not restrict, exclude or limit any duty or liability to any person under any applicable laws or regulations of any jurisdiction which may not be lawfully disclaimed. The information in this document is confidential and proprietary to RBS and is intended for use only by you and should not be reproduced, distributed or disclosed (in whole or in part) to any other person without our prior written consent.

The Royal Bank of Scotland plc. Registered in Scotland No. 83026. Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB. The Royal Bank of Scotland plc is authorised by the Prudential Regulation Authority, and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.