Begin

Business On Line

Customer Handbook

Bank of Ireland UK

Contents

Section 1. Business On Line

1.1. Benefits of Business On Line

Business On Line is a versatile, easy to use and cost effective way to manage your daily banking needs and is accessible from any device with internet access. This includes limited access through a mobile phone or tablet device where you can view account balances, transaction history and details of payments made.

Advantages of using Business On Line (BOL) for your daily banking needs:

a. Reduce the time spent making telephone calls to the branch for balances, transactions and doing cheque searches. Balances and transactions can be viewed throughout the day, transactions can be filtered to find specific information.

b. Reduce your time writing and posting cheques by paying your customers, clients and employees on Business On Line. Payments can be post-dated for up to 60 days, allowing you to set-up payments, wages prior to going on business trips or holiday, these can be cancelled up to one day prior to the payment date, subject to cut-off times.

c. Make account transfers throughout the day with instant effect Transfer money to any of your own business accounts and use those funds with immediate value.

d. Reduce paper work in the office. All Business On Line transactions are stored electronically for 90 days and can be accessed and/or printed at any time to accommodate company account reconciliation.

e. Customise Business On Line to meet your company's needs. Give your accounts nicknames to match your filing structure, allow as many Authorised Users as you wish to access the system and control exactly what each person can do.

f. Business On Line uses quality internet security, combining high end encryption and Two Factor Authentication (User ID's, passwords (including those generated by the Approve app) and One Time Activation Codes (via SMS)

g. Allow Third Party Providers (TPPs) to access information about your bank account and make payments on your behalf.

1.2. Services

- View balances of single accounts or several accounts simultaneously.
- View and perform searches on transactions for the previous 90 days (90 day bank statement).
- View Credit Card Account balances and transactions.
- Make Credit Card Payments.
- Perform a cheque search.
- Rename accounts for ease of use on BOL.
- Make "Account Transfers" between accounts on BOL.
- Make payments to any person and/or business in BOI or non-BOI accounts within your jurisdiction. ("Third Party Payments").
- Make bulk (EFT/ BACS*) Payments, including; Payroll for Employees (Direct Pay), pay creditors using Direct Credit and collect Direct Debits from customers.
- Future-dated payments (e.g. if away on holiday post-date several weeks wages in advance of leaving).
- Payments can be cancelled or amended up to one day prior to the date they are due to occur.
- Stop a cheque.
- Store up-to 200 employees/clients/customers bank details for easy access when making payments. Inactive payee details will be removed after 2 years.
- Transaction details and payment details can be printed with a 90 day history for the customers own use (e.g. reconciling their account books).
- An Audit trail is provided for Administrator(s) to monitor user activity.
- Make International "Account Transfers" and "Third Party Payments" to anywhere in the world.
- View transaction details on currency accounts held within your jurisdiction.
- View Treasury Deposit accounts.
- Make urgent (same day) payments to BOI and non-BOI accounts.
- Export the 90 day account statement to your computer in different formats so you can sort and filter the data as you wish.
- View interest accrued, both debit and credit, on branch banking accounts and Global Market bank accounts.
- TPPs can access your account (if they are registered with their banking regulator) provided they have your consent which you have verified using our online verification processes and Security Instruments. If you don't want to allow anyone else access to your account, you don't have to.

*Please note the EFT /BACS function requires a Credit Limit to be agreed by the Bank. In the event of a file of payments being submitted the value of which is higher than the credit limit approved, the file will be rejected and not processed. Lending criteria and terms and conditions apply.

Section 2. Customer support

Business On Line is designed to be as user friendly as possible. In order to help you find your way around Business On Line with ease, a number of support services have been developed.

2.1. Learning Centre

We provide support and training to all Business On Line customers through our Learning Centre, which includes the Business On Line Training Portal and Online Training Videos.

The Training Portal consists of training lessons and videos, incorporating a "show me, try me" concept, and the option to pause and replay throughout. The Portal will take you through the initial set up and functionality of Business On Line.

To view the Business On Line Learning Centre, please click on the Training Portal icon on the Business On Line home page, or through the Learning Centre link on the bottom left hand corner of the Dashboard under Quick Actions.

2.2. Customer Support Unit

If an Authorised User experiences difficulties with Business On Line, having consulted the Learning Centre, they should inform their Business On Line Administrator(s). If the Administrator(s) are unable to solve the problem, the Bank's Customer Support Unit is available to answer queries. This service is free of charge to Business On Line Customers.

The Customer Support Unit is open from 9:00am to 5:00pm, Monday to Friday (excluding Bank Holidays). Contact details are available on the Business On Line website.

2.3. Problem Solving Procedures

If a problem exists:

a. View Help and Support Page

b. Interactive Training Portal available on the BOL website

c. Contact the Administrator(s)

- If problem persists, or if Authorised User cannot find a solution, contact the Administrator(s).

d. Contact Customer Support Unit

- If problem remains unresolved contact Customer Support Unit. Contact details are available on the BOL website.

Section 3. Technical specifications

Operating Systems and Browsers:

To optimise performance and comply with the latest security standards, computers and internet browsers used to access Business On Line must meet minimum system requirements. You can view the latest requirements on our website boi.com/boltechnicalspec.

Mobile Phone

A mobile phone is required to receive service related messages. Some examples of where we might send SMS messages include:

1) an Authorised User creates a payee;

2) for Administrator(s) to receive an activation code to complete the set up of their Business On Line profile.

3) to communicate important service information or

4) if we are believe that the security of your account is compromised.

Smart Mobile Device

All customers will be required to have a smart mobile device in order to download the Approve app.

- We recommend that customers operate their smart mobile devices on the latest software version. More information on device compatibility can be found on our website, boi.com/boltechnicalspec

Section 4. System security

4.1. The Internet

The customer is responsible for making absolutely sure that they have put in place reliable internet security systems (e.g. industry standard, up to date, supported and licensed anti-virus software).

These are vital to prevent:

- Unauthorised access to a Customer's computer system and smart mobile devices.
- Unauthorised disclosure of sensitive information.
- Any possible tampering with systems or the data on them.
- Disruption of services due to Internet access problems.

4.2. Banking Security Encryption System Design

We protect the confidentiality of data being transferred between the bank and the Customer using 128 bit encryption which is a sophisticated form of data encryption and to ensure only intended users can read the information.

Customers accessing BOL, authorising payees and making payments must be registered to use the Approve app.

In addition to this, The Bank through a variety of internal security controls protects BOL and any data processed through it.

4.3. One Time Passwords

The Approve app is a Security Instrument which generates One Time Passwords (OTP) which will need to be input alongside your username to log in to Business On Line. These One Time Passwords will be required regardless of whether a user is an Administrator or a standard Authorised User.

Administrators and Authorised Users will also be prompted to input a One Time Password to undertake certain activities using Business On Line. For example to create a payee, and set up or approve payments.

4.4. Security Codes

We will send Security Codes (One Time Activation Codes) via SMS to registered Administrator mobile phones:

- Where Administrators are activating their Approve app for the first time, or;
- Administrators are registering their existing Approve app to another Business On Line profile

The Administrator(s) are responsible for providing Bank of Ireland with a valid mobile phone number to accept delivery of the One Time Activation code

4.5. Customer Security

4.5.1. Administrator(s)

a. BOL is designed to give Customers a high level of control over their own financial affairs, reducing reliance on the Bank for general administration of the service. This increased level of autonomy allows for greater control and provides efficiencies for the customer.

b. The role of the Administrator is a fundamental feature of the system and may differ from other electronic banking systems in existence.

c. The Customer must satisfy itself as to the integrity and suitability of the person(s) whom it has chosen as Administrator(s).

d. The person(s) appointed as Administrator(s) at the Customer site is/are responsible for setting up Authorised Users and has full responsibility for the level of access provided to Authorised Users.

e. If a Customer appoints two Administrators, both Administrators will have to perform the Services together (they share a dual log on).

4.5.2. Role of the Administrator(s)

a. The Administrator(s) control who has access to the service and what their Authorised Users are permitted to do.

b. The Administrator(s) register and maintains all Authorised User Details on BOL

c. The Administrator(s) issue Authorised User IDs and enables the Approve app for the other Authorised Users

d. The Administrator(s) can at any stage prevent an Authorised User from logging onto the system.

e. The Administrator(s) controls the Authorised Users' ability to prepare and authorise payments.

f. The Administrator(s) are responsible for making the Authorised User aware of their responsibility to check the status of pending payment instructions on the system.

The Audit Log shows a list of the critical actions performed by Administrator(s).

4.5.3. Responsibility of Administrator(s)

To log-on to the Administrator function, it is necessary for the Administrator's Approve app One Time Password to be entered. Thereafter all Administrator functions can be performed by the Administrator(s). The Administrator function should be exited immediately once the necessary duties have been performed.

g. It is the responsibility of the Administrator(s) to ensure that a review of the customer audit log takes place on a regular basis. The customer audit log records changes made by the Administrator(s) to the identity and access levels of Authorised Users

h. If an irregularity is identified, the Administrator(s) should verify the authenticity of transactions with the relevant Authorised Users. If there is still concern regarding irregularities, you must notify the Bank immediately. You can do this free of charge via the number listed on bankofirelanduk.com.

i. Once training is provided by the Bank, i.e. Training Portal, Phone and WebEx it is the Administrator's responsibility to train all other new and existing Authorised Users.

j. It is solely the responsibility of the Administrator(s) to communicate company guidelines on the use of BOL to the Authorised Users and to ensure compliance with those guidelines. Given the level of responsibility held by Administrator(s), we strongly recommend that a member of the Customer's senior management should review their activities on a regular basis, including reviewing these activities on the audit log.

4.5.4. Password Protection

One Time Passwords generated for use on BOL are unique to the function that is being carried out. Passwords do not need to be retained for future use. Unauthorised personnel should not be able to gain access to a password.

For more details refer to the 'Security Guidelines' available on the Customer website.

Where you use your Security Instrument with a TPP to interact with BOL on your behalf, you must only share such details with a TPP who holds an appropriate authorisation from the relevant regulatory authorities to provide payment services in respect of your account(s).

4.5.5. Reducing the Risk of Fraud

Businesses and organisations are increasingly becoming targets of fraud and cybercrime. There are a number of procedures that Customers can put in place to reduce the risk of exposure to fraud:

4.5.5.1. Seniority

The Administrator(s) should be either a senior manager or report directly to one. The Administrator(s) is in charge of BOL on the Customer's site and is solely responsible for granting or denying access to it by authorised personnel and the ability of Authorised Users to initiate or authorise payments. When a Customer Administrator sets up and assigns a role to an Authorised User, the Bank will accept transactions from that Authorised User in good faith and act on them accordingly. As a result, Customers are liable for transactions carried out using their Security Instruments (subject to any exclusions set out in the Conditions of Use).

4.5.5.2 Segregation of Duties

Things to remember when setting up your Business On Line profile:

a. **Apply the minimum access necessary**
Apply the minimum access necessary for each user to undertake their duties. You can create multiple User Groups with different 'tiers' of access. Be particularly selective about which employees are granted access to authorise payments, for example - only those employees of a supervisor or manager level.

b. **Split responsibilities**
Split the responsibility to initiate a transaction from the responsibility to authorise it, so that no one person can do both. This helps to validate that the information being entered and acted on is correct.

c. **Dual authorisation**
Require two different people to authorise payees and payments. This adds a '4-eye' checkpoint to confirm the accuracy and authenticity of each request, at each step in the payment journey.

d. **Establish authorisation limits**
Use the authorisation limits on Business On Line (also known as payment panels) to require that higher value payments are authorised by specific authorisers, or multiple authorisers.

e. **Set a realistic Daily Control Limit**
Set a Daily Control Limit on the profile which is commensurate with your payment requirements. Always apply the lowest tolerable figure and review this regularly to ensure it remains relevant to your requirements. Where this figure needs to be raised, consider requesting a temporary increase to cover a specific time period.

Reminder: Your Daily Payment Control Limit is the maximum amount you can send to third parties on Business On Line on one day. It is an important control measure and you should set it to an appropriate figure for your payment requirements

f. **Unique Users**
Always ensure every user has their own unique username for logging on to Business On Line. This allows traceability of actions completed in the channel and transparency as to who executed them.

g. **Conduct regular training**
Conduct regular training with your staff on the threats to your business, ensuring they are aware of the new and persistent risks and how they can occur outside of the workplace and work environment. We have a range of supports available at bankofirelanduk.com/help-and-support/security-and-fraud/ that will help you prevent financial loss due to fraud.

4.5.5.3. Control Access

Physical, logical and network access should be stringently controlled on all devices used for BOL.

Logical access should be controlled by use of a 'power-on password'. (Consult the device operating manual for details). It is better to use a secure operating system that incorporates strong logical access control, such as Windows NT configured for security. (It is important to note that if NT is configured with default settings it may not provide sufficient security.) This should be confirmed with your technology supplier.

Network access controls should be in place to ensure network integrity before connecting to BOL Such controls should cover, for example, network administration, audit trail review and change management procedures. None of these controls individually will provide comprehensive security, but working together they can help to create a secure electronic banking environment.

None of these controls individually will provide comprehensive security, but working together they can help to create a secure electronic banking environment.

4.5.5.4. Knowledge of Procedures

Customers should make sure that all staff using BOL understand that the procedures are issued for their own protection, as well as for the protection of the customer. Customers should also ensure, for their own protection, that the procedures in this handbook are strictly adhered to, as any deviation (e.g. sharing of a username) could expose the Customer to internal fraud.

4.5.5.5. Report Deviations from the Norm

There should be a logical explanation for everything that occurs on BOL and any deviation or unexplained event should be reported immediately to senior management and to the Bank.

4.5.5.6. Updating Procedures

Ensure that there is a procedure for setting up and removing access to BOL. From time to time people move jobs and their responsibilities change. All information should be current.

4.5.5.7. Daily Control Limit

The daily control limit limits the overall value of payments (excluding SEPA Bulk or BACS payments, Domestic Account Transfers and International Account Transfers) that can be authorised on a BOL profile. The Administrator(s) can amend the daily control limit by contacting the Business On Line Help Desk.

Section 5. Hints and tips

The Do's:

a. Remember to use the help and support facilities if in any doubt.

b. Use BOL facilities as extensively as possible for maximum benefit.

c. Call the BOL Support Team with any feedback regarding BOL. Customer contact details are available on the customer website or E-mail: businessonlineuk@boi.com.

d. Exit BOL before visiting other sites on the Internet.

e. Keep your Security Instruments safe and secure and notify the Bank immediately if they are compromised.

The Don'ts:

f. Don't allow unauthorised personnel access to BOL under your Security Instruments.

g. Don't use obvious Passwords.

h. Don't forget the deadlines for sending payments which are outlined under the Help and Support section on our website businessonline-boi.com.

i. Don't leave your device unattended if you are logged into BOL.

j. Don't leave your registered mobile device unattended if you are logged into BOL.

k. We recommend that you don't access Business On Line from the same device that you use the Approve app on for authentication.

Section 6. Maintenance

From time to time the Bank will need to carry out essential maintenance to BOL. Other than in exceptional cases, this will be restricted to the hours of 19.00 hrs to 07:00 hrs.

Section 7: Bank safely – Fraud Awareness information

Be wary of any request that asks you to make a payment, to change bank account details or asks for remote access to your laptop/device. It could be fake, so double check it's legitimate.

Pick up the phone and give them a call. Always make sure it's a phone number you already have for them - don't use a phone number given to you in the message.

Contact Bank of Ireland UK immediately on the details below to report online fraud, if you have disclosed any information following a suspicious email, text or call, or you have any concerns regarding your account.

UK Freephone: 0800 032 1288

From abroad: +353 56775 7007

Available 24 hours, 7 days a week.

For more information on how to protect yourself from fraud, search 'Security and Fraud' on our website bankofirelanduk.com and follow us on Twitter @BankofIrelandUK

Remember: Bank of Ireland UK will **never** ask for account information or any of your security credentials, including one-time codes you generate. One time codes are provided to protect you from fraud, so do not give codes to anyone, no matter who they say they are or why they say they need it. We will never send you a text message or email containing a direct link to a logon page.

We can provide this document in Braille, in large print and on audio tape.

Please ask any member of staff for details.

UK37-1338N.11 (09/24)

Bank of Ireland UK