Begin

Business On Line

Customer Handbook
April 2021

Bank of Ireland

Contents

Part 1: Business On Line

Section 1. General

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. (Business On Line is available on mobile phone and tablet devices where customers can view their 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 & transactions can be viewed throughout the day; transactions can be filtered to find specific information.

b) Reduce your time writing & posting cheques by paying your customers, clients & 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 holidays; these can be edited or cancelled up to one day prior to the payment date, subject to cut-off times.

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

d) Reduce paperwork 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 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 (passwords (including those generated by KeyCode), and one time authentication codes (via SMS)).

g) Allow Third Party Providers (TPP) 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 payments to Credit Cards
- Perform a cheque search
- Rename accounts for ease of use on BOL
- Make "Account Transfers" between your accounts on BOL
- Make payments to any person and/or business in BOI or non-BOI accounts within your jurisdiction ("Third Party Payments")
- Make non urgent payments to any person and/or business in BOI or non-BOI accounts within your jurisdiction ("Third Party Payments") or make SEPA credit transfer (ROI customers only)
- Make BACS Payments (UK Customers only), including; Payroll for Employees (Direct Pay),pay creditors using Direct Credit and collect Direct Debits from customers through manual key-entry or file upload (Import)
- Conversion Services (ROI customers only) provides the conversion of SEPA Bulk payment file format ('Standard 18' as per Bank of Ireland's published version) for credit payments to SEPA (XML) format and onward processing into SEPA. These services include the enrichment of account details (NSC and account number) to IBAN and BIC
- 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 two days 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
- Third Party Providers (TPP) can access your account if they are registered with their banking regulator and have your consent which you have verified using our online verification processes and your security instruments. If you don't want to allow anyone else access to your account, you don't have to.
- Make Same Day Money Transfer (SDMT/ CHAPS) to BOI and non-BOI accounts

- Export the 90 day account statement to your computer in CSV format so you can sort and filter the data as you wish
- Interest accrued, both debit and credit, on branch banking accounts and Global Market bank accounts

Please note the SEPA (ROI) /BACS (UK) 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 & conditions apply.

Section 2. Customer Support

Business On Line is designed to be as user friendly as possible. In order to help the Customer find their 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 our Help & Support page and Training Portal.

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 interactive Training Portal and other help and support documentation, 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. If the Administrator is 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 8:00am to 6.00pm, 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:

1. View Help & Support Page
2. Interactive Training Portal available on the BOL website
3. Contact the Customer Administrator(s)

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

4. Contact Customer Support Unit

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

Section 3. Technical specifications

Operating Systems and Browsers:

To optimise performance and comply with the latest security standards, equipment, operating systems and internet browsers used to access Business On Line must meet minimum requirements. You can view the latest requirements on our website.

Mobile Phone

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

- for an Administrator to receive an activation code to begin their set up of the KeyCode solution
- to communicate important service information or
- if we are suspicious 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 Bank of Ireland KeyCode App. Compatible devices for the Bank of Ireland KeyCode App are any smart mobile device, including iOS, Android or Windows smartphone, tablet or iPod Touch. No internet access is required post-download.

Section 4. System Security

4.1 The Internet

The customer is responsible for making sure that they have put in place reliable internet security systems (e.g., anti-virus software).

These are vital to prevent:

- Unauthorised access to a Customer's computer system / 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 System Design

We protect the confidentiality of data being transferred between the bank and the Customer by using 128 bit encryption which is a sophisticated form of data encryption.

1. Encryption ensures only intended users can read the information.
2. Customers accessing BOL, authorising payees and making payments must be registered to use KeyCode; a secure software application which provides one time passwords.
3. The Bank through a variety of internal security controls protects BOL and any data processed through it.

KeyCode - One Time Password

The KeyCode Token / one-time password (OTP) security instrument is required for all users in order to access Business On Line. Users will require this security instrument whether they are an administrator or a standard BOL user.

The user will enter their username and then will generate a one-time Password (OTP) on their mobile application which will be inputted on the homepage to access Business On Line. Administrators and Users will also be prompted to input a one-time password generated by KeyCode to undertake certain activities using Business On Line. For example a one-time password will be required to:

- Authorise and cancel payments
- Authorise a payee

The KeyCode software application will require a one-time registration code to be entered to enable the application on first use.

Security Codes

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

- where Administrators are activating their KeyCode App for the first time or
- Administrators are registering their existing KeyCode App to another Business On Line profile

The Administrator is responsible for providing Bank of Ireland with a valid mobile phone number to accept delivery of the One Time Authentication code

4.3 Customer Security

4.3.1 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(s) 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 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) We recommend the appointment of two Administrators. Administrators should be co-located as they will share a dual logon.

4.3.2 Role of Administrator

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

b) The Administrator registers and maintains all Authorised User Details on BOL

c) The Administrator issues Authorised User IDs (and enables KeyCode) to the other Authorised Users and can at any stage or prevent an Authorised User from logging onto the system.

d) The Administrator controls the Authorised Users' ability to prepare and authorise payments as well as their individual authorisation limits. They must make the Authorised Users aware of their responsibility to check the status of pending payment instructions on the system.

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

4.3.3 Responsibility of the Administrator

a) To log-on to the Administrator function, it is necessary for the Administrator's KeyCode one time password to be entered. Thereafter all Administrator functions can be performed by the Administrator. However, as a matter of company policy, you may wish to require that both Administrators are present for the discharge of all functions. The Administrator function should be exited immediately once the necessary duties have been performed.

b) It is the responsibility of the Administrator 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 to the identity and access levels of users.

c) If an irregularity is identified, the Administrator should verify the authenticity of transactions with the relevant Authorised Users If there is still concern regarding irregularities, the Bank's Customer Support Unit should be contacted immediately.

d) Once training is provided by the Bank, i.e., phone or portal, it is the Administrator's responsibility to train all other Authorised Users, including both existing and new Authorised Users.

e) It is solely the responsibility of the Administrator to communicate company guidelines on the use of BOL to the Authorised Users and to ensure compliance with those guidelines.

f) Given the level of responsibility held by an Administrator, we strongly recommend that a member of the Customer's senior management should review the activities of the Administrator on a regular basis, including reviewing these activities on the audit log.

4.3.4 Password Protection

KeyCode passwords generated for use on BOL are unique to the function that is being carried out. Keycode 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 acount(s).

4.3.5 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:

4.3.5.1 Administrator Seniority

The Customer Administrator should be either a senior manager or report directly to one. The Administrator 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).

4.3.5.2 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: The Daily Control Limit is the maximum sum of all payments that can be authorised on a given day (excluding own account transfers and instructions within bulk files).

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 boi.com/security-zone that will help you prevent financial loss due to fraud.

4.3.5.3 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. 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.

4.3.5.4 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.

4.3.5.5 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.

4.3.5.6 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.

4.3.5.7 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. An Administrator can amend the daily control limit by contacting the Business On Line Help Desk.

Section 5. Dos and Don'ts

Dos:

a) Remember to use the 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: business.online@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.

Don'ts:

a) Allow unauthorised personnel access to BOL under your security instruments.

b) Use obvious Passwords

c) Don't forget the deadlines for sending payments which are outlined under the Help and Support section on our website www.bankofireland.com

d) Don't forget to review the Audit Log regularly to monitor activity on BOL.

e) Leave your device unattended if you are logged into BOL.

f) We recommend that you do not access Business On Line from the same device that you use the Bank of Ireland KeyCode 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: Protect your Business against Fraud

Fraudsters can send convincing letters or emails pretending to be a colleague (including senior executives such as the CEO) or supplier and attempt to trick you into making a payment to a fraudulent account. Always verify with a known contact that the request and/or the account details are genuine.

Please immediately contact Bank of Ireland on the below details to report online fraud, suspicious activity or unauthorised transactions on your account, or if you have disclosed any information in error following a suspicious email, text or call:

ROI Freephone: 1800 946 764

From abroad: +353 56775 7007

Available 24 hours, 7 days a week.

Visit boi.com/security-zone for more information about how you can protect your business.

REMEMBER: Bank of Ireland will never ask for account information or to share a password generated by your Keycode App. We will never send you a text message or email containing a direct link to a logon page.

Part 2: Business On Line Payments Plus (ROI only)

Section 1. General

1.1 Benefits of Business On Line Payments Plus

Business On Line Payments Plus (BOL Payments Plus) is a versatile, easy to use efficient method of submitting and processing bulk files in SEPA XML formats and accessing associated reports.

The advantages of using BOL Payments Plus for your SEPA file processing include:

a) Participation as a creditor (an originator) in the SEPA Direct Debit scheme allows for the easy collection of funds from clients and customers across the SEPA countries.

b) Reduce paperwork in the office. All BOL Payments Plus reports are available online. These include file rejection reports and creditor settlement reports. These reports can be accessed and/or exported at any time to accommodate company account reconciliation.

c) BOL Payments Plus utilises quality internet security, and a combination of strong authentication through the use of a physical security device – a Digipass* or a Keycode App – protected by a user unlock code which generates one-time passwords.

1.2 Available Functionality

Reporting Information in relation to file rejections and returned payments can be viewed, exported and printed easily using Business On Line Payments Plus and/or the Bank of Ireland Business On Line File Gateway (BOLFG) portal.

- A creditor settlements report available to Direct Debit customers, to facilitate bank account reconciliation.
- Submit SEPA bulk file payments
- Future date payment files for up to 60-days in advance of payment.
- Payments can be cancelled up to two day prior to the date they are due to occur.

Section 2. Customer Support

Business On Line Payments Plus is designed to be as user friendly as possible. In order to help the Customer find his/her way around BOL Payments Plus with ease, a number of support services have been developed, including an online Demo and FAQ's, this information is available on the homepage.

2.1 Contextual Help

Contextual on-screen help accompanies various functions throughout BOL Payments Plus In order to solve problems and to enhance understanding of the meaning of these functions.

2.2 Customer Support Unit

The Customer Support Unit is open from 8:00am to 6.00pm, Monday to Friday (excluding Bank Holidays). Contact details are available on the BOL Payments Plus website.

2.3 Additional Support

In the event that the problem cannot be solved over the phone, a further level of support is available which may involve a site visit. This support may be available on request and may involve a charge in order to cover costs, details of which are available on request from the Customer Support Unit.

2.4 Problem Solving Procedures

If a problem exists, the following support options are available to assist:

1. An online demonstration is available on the BOL Payments Plus homepage
2. Contextual on-screen help text
3. Help and Support Section on the BOL Payments Plus homepage
4. FAQ's on the BOL Payments Plus homepage
5. Contact customer support unit.

Section 3. Technical specifications

Operating Systems and Browsers:
To optimise performance and comply with the latest security standards, equipment, operating systems and internet browsers used to access Business On Line File Gateway and Business On Line Payments Plus must meet minimum requirements. You can view the latest requirements on our website.

Section 4. System Security

4.1 The Internet

The customer is responsible for making sure that they have put in place reliable internet security systems (e.g. anti-virus software).

These are vital to prevent:

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

4.2 Business On Line File Gateway

Business On Line File Gateway (BOLFG) is the means by which SEPA files (in XML format) can be transmitted to Bank of Ireland. The Bank has a Business On Line File Gateway for this purpose. In order to upload a SEPA payments file using the Business On Line File Gateway, a user must possess a User ID and password. These credentials are issued by the Bank to one of the administrators of the associated BOL profile.

4.3 Bank Security Instruments

4.3.1 Digipass

A Digipass is a physical device that is used to authenticate the identity of the BOL Payments Plus user in order to securely authorise a SEPA file for processing. Each Digipass provides user access to BOL Payments Plus and the capability to authorise SEPA files for a single SEPA Originator number.

At the outset, the Digipass is sent to one of the administrators (if two administrators are in place) on the associated Business On Line profile. In order to complete registration of the device to the SEPA originator number, the administrator must telephone the BOL Payments Plus Customer Support Unit. The Digipass holder sets a five-digit PIN without which the Digipass cannot be operated. This PIN is required in order to gain access to the Digipass and if this code is lost or forgotten, a replacement device will need to be sent out by post resulting in a potential delay to the processing of SEPA payment files.

4.3.2 KeyCode - One Time Password

The KeyCode Token / one-time password (OTP) security instrument is required for all users in order to access the application.

The user will enter their username and then will generate a one time Password (OTP) on their mobile application which will be inputted on the homepage Business On Line Payments Plus log-in page to access Business On Line Payments Plus. Administrators and Users will also be prompted to input a one time password generated by Keycode to undertake certain activities using Business On Line Payments Plus. For example a one time password will be required in order to securely authorise a SEPA file for processing

The Keycode software application will require a one-time registration code to be entered to enable the application on first use which will be provided by the Bank.

4.3.3 Logon

Access to BOL Payments Plus is by way of a one-time password which is generated by the Digipass or the KeyCode App which is entered on the BOL Payments Plus Logon Homepage.

4.3.4 File Transmission

Before a SEPA payments file can be authorised on BOL Payments Plus, the file must first be transmitted to the bank. This is typically done through the Bank of Ireland Business On Line File Gateway (File Transfer protocol). For further information in relation to the Business On Line File Gateway solution, please see section 4.2 and consult the training solutions available on the BOL Payments Plus homepage.

4.3.5 File Authorisation

SEPA payment files must be authorised before the payments/collections will be processed. A transmitted file may be broken into constituent batches. A file may comprise of multiple batches if payments are originating from more than one payer/creditor account and/or have multiple value dates.

After logon, the Digipass / KeyCode App holder performs some cross checking activities in relation to the file details available on screen. The authorisation is completed by entering a Message Authentication Code (MAC) when using the Digipass or the Challenge Code or a Payee / Import File Code' when using the KeyCode App.

4.4 Customer Security

4.4.1 Administrator(s)

a. The role of the Administrator(s) for BOL Payments Plus is key to the authorisation authority for the transmission of payment files.

b. The customer must satisfy itself as to the integrity and suitability of the person whom it has chosen as Administrators.

c. The person(s) appointed as Administrator(s) on the BOL Payments Plus profile has responsibility for transmission and authorisation of payment files. An Administrator may choose to authorise payment files or nominate a user of appropriate level of authority with the organisation to discharge these responsibilities.

d. We recommended the appointment of two Administrator(s)

e. User Logon credentials and the Security Instruments should be held with the utmost care and security.

f. Loss of the User Logon and/or Security Instruments can result in a delay of a number of days while replacement(s) are generated and delivered by post.

4.4.2 Role of Administrator

4.4.2.1 Digipass

a. The Administrator controls are responsible for the transmission and authorisation of SEPA files. Where the role of the administrator is shared by two individuals, the responsibility for the tasks of Business On Line File Gateway transmission and authentication will be segregated between the two.

4.4.2.2 KeyCode

a. The administrator controls who has access to the Business On Line Payments Plus service and which Authorised users can authorise a payment file.

b. The Administrator enables KeyCode for Authorised Users and can at any stage or prevent an Authorised User from logging onto the system.

4.4.3 Segregation of Duties

BOL Payments Plus allows you to segregate duties within your company. One user can be responsible for uploading bulk files via Business On Line File Gateway and a second user can have responsibility of authorising all uploaded files.

4.4.4 Password Protection

4.4.4.1 Digipass

It is essential that the Digipass PIN is managed securely. It is your organisation's responsibility to ensure that Digipass PIN is not disclosed to unauthorised personnel. For more details refer to the 'Security' and 'Privacy policy' details available on the BOL Payments Plus website.

4.4.4.2 KeyCode App

It is essential that any PIN protecting the KeyCode App is managed securely.

KeyCode passwords generated for use on BOL Payment Plus 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.

4.4.5 Use of Passwords

The administrator creates the initial Digipass PIN or KeyCode App PIN

a. The Bank will not have knowledge of this PIN and therefore the customer has full responsibility for remembering it.

b. The Digipass PIN will revoke after 9 unsuccessful logon attempts and the KeyCode App PIN will revoke after 5 unsuccessful logon attempts.

c. The Bank cannot reset the Digipass PIN and in this instance a new device must be ordered. In the event of a lost or stolen Digipass or PIN, the Bank must be notified immediately and a new device must be ordered by calling the BOL Payments Plus Customer Support Unit. It may take a number of days before a replacement device is received.

d. In the event of a lost or stolen KeyCode App or PIN, the Bank must be notified immediately by calling the BOL Payments Plus Customer Support Unit.

4.4.6 Reducing the Risk of Fraud

There are a number of procedures that Customers can put in place to reduce the risk of exposure to fraud.

4.4.6.1 Seniority

Your organisation has responsibility for BOL Payments Plus at your own 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 Files. If possession of a Security Instrument is transferred to an alternative user, the Bank will not be aware and will accept transactions from that user in good faith and act on them accordingly. As a result, your organisation is liable for all transactions carried out on the BOL Payments Plus channel (subject to any exclusions in the Conditions of Use). To limit exposure to fraud your organisation is advised to separate the roles of Business On Line File Gateway upload of files from the role of authoriser on BOL Payments Plus.

4.4.6.2 Control Access

Physical, logical and network access should be stringently controlled on all devices used for BOL Payments Plus. 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. This should be confirmed with your technology supplier. Network access controls should be in place to ensure network integrity before accessing BOL Payments Plus. Such controls should include, 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.

4.4.6.3 Knowledge of Procedures

Your organisation should ensure that all staff using BOL Payments Plus understands that the procedures are issued for their own protection, as well as for the protection of the organisation. You should also ensure, for the protection of the organisation, that the procedures and recommendations in this handbook are strictly adhered to, as any deviation (e.g. sharing of Security Instruments such as passwords, PINs or Digipasses) could expose your organisation to Internal fraud.

4.4.6.4 Report Deviations from the Norm

There should be a logical explanation for everything that occurs on BOL Payments Plus and any deviation or unexplained event should be reported immediately to senior management and, if concerns still persist, such events should be raised to the BOL Payments Plus Customer Support Unit.

4.4.6.5 Updating Procedures

From time to time people move jobs and their responsibilities change. You organisation should ensure that sufficient procedures are in place for managing and transferring access to BOL Payments Plus and the Business On Line File Gateway.

Section 5. Dos and Don'ts

Dos:

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

b) Use BOL Payments Plus facilities as extensively as possible for maximum benefit.

c) Call the BOL Payments Plus Support Team with any feedback regarding BOL Payments Plus. Customer contact details are available on the customer website.

d) Exit BOL Payments Plus before visiting other sites on the Internet.

e) Use the Demo on our homepage.

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

Don'ts:

a) Allow unauthorised personnel access to Business On Line File Gateway or BOL Payments Plus under your Security Instruments.

b) Forget the deadlines for sending payments which are outlined on our website.

c) Leave your device unattended if you are logged into BOL Payments Plus.

Section 6. Maintenance

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

Bank of Ireland is regulated by the Central Bank of Ireland.

Bank of Ireland

37-1436R.1 (04/21)