Business On Line

Customer Handbook

January 2018

Bank of Ireland

For small steps, for big steps, for life

Contents

Part 1: Business On Line (ROI only)

Section 1. General

1.1. Benefits of Business On Line.

Business On Line: The Business Banking Solution

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 are live and 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 (User IDs, passwords, and one time authentication codes (via SMS)).

1.2. Services

- View up-to date balances of single accounts or several accounts simultaneously
- View and perform searches on transactions for the previous 90 days (90 day bank statement)
- View "Standing Orders" and "Direct Debits" on registered accounts (UK Customers only)
- 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
- 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 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 Learning Centre icon on the Business On Line home page, or through the 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 Customer Administrator
   - If problem persists, or if Authorised User cannot find a solution, contact Customer Administrator(s).
4. Contact Customer Support Unit
   - If problem remains unresolved contact Customer Support Unit. Contact details are available

Section 3. Technical specifications

Operating Systems

Windows 7, 8, 8.1 & 10
MAC OS X 10.7 (or higher)

Java

Latest version from www.java.com

Browsers

Optimised for:
Internet Explorer Versions 9, 10, & 11
Latest versions of Firefox and Safari

Where a Customer has not yet migrated to KeyCode , the following will prevent Business On Line from working correctly:

- Some network firewalls may prevent Business On Line from working correctly
- No working Java / out-of-date Java on the PC
- Logging on through Metro mode (Windows 8).

Access

Business On Line uses Java-based programmes and as such will not be available to devices that have protective firewalls configured to reject Java (applet) requests. Please contact us in order to overcome this problem (if you have not migrated to the KeyCode solution).

Mobile Phone

A mobile phone is required… (1) an Administrator using the Digital Cert solution authenticates a User with payee authorisation rights; or (2) a User creates or edits a payee; or (3) An Administrator requires an activation code to begin their set up of the KeyCode solution.

Smart Mobile Device

All customers upon migrating to KeyCode solution 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 Encryption System Design

There are three specific security measures which, when working together, provide an exceptional level of security.

1. We protect the confidentiality of data being transferred between the bank and the Customer by using encryption.
   - This involves 'scrambling' information using 128 bit encryption which is a sophisticated form of data encryption data and only intended users can read the information.

2. Customers making payments by BOL have a second level of security.

This second level of security will depend on whether a Customer will be using KeyCode or Digital Certificates as a security measure. The following applies depending on which method is used.

Digital Certificate

A "Digital Cert" and a "Digital Cert Password" are created by the customer on a particular PC.

- The "Digital Cert" is retained securely by the bank
- The "Digital Cert Password" is retained by the customer and used to authorise each payment
- Even though you can access BOL from any PC any where in the world the "Digital Cert Password" is PC specific and will only work on the particular PC that it is set up on
- The "Digital Cert Password" is a key that is verified by the "Digital Cert" held within the bank each time a transaction is made
- Each certificate is uniquely linked to an individual user and a change to the identity requires the issuance of a new certificate

KeyCode - One Time Password

The Token / one-time password (OTP) solution will apply for all users in order to access the application. Users will require this solution whether they are an administrator or a standard BOL user.
The user will enter their username and then will generate an OTP on their mobile application which will be inputted on the homepage to access Business On Line.

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

3. The Bank through a variety of internal security controls protects BOL and any data processed through it.

4.3 Two Factor Authentication

There is an additional layer of security on Business On Line, namely Two Factor Authentication, for the following two scenarios:

a. An Administrator creates or edits a User with payee authorisation access rights on Business On Line (for customers using Digital Certificates as a security measure only)

- The Administrator will receive a One Time Authentication code to their registered mobile phone when creating/editing users they provide payee authorisation access rights to.
- The Administrator is responsible for entering the One Time Authentication code on Business On Line.
- The Administrator is responsible for providing Bank of Ireland with a valid mobile phone number to accept delivery of the One Time Authentication code.

b. A User creates a new payee or edits an existing payee on Business On Line (for Customers using Digital Certificate or where KeyCode is restricted to password and payment functionality only).

- The User will receive a One Time Authentication code to the registered mobile phone when they select authentication of a Payee.
- The User is responsible for entering the One Time Authentication code on Business On Line.
- The User may change their registered mobile phone number by contacting the Administrator(s).

4.4 Customer Security

4.4.1 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. To facilitate this (where Digital Certificates are used), a unique Administrator password will be issued at the time of log on to each Administrator.

f) (Where Digital Certificates are used) , each Password should be treated with the utmost secrecy and confidentiality. These Passwords are system generated; therefore if one is forgotten or lost a new one will have to be issued by the Bank.

g) (Where Digital Certificates are used) , this may result in delays of at least three working days for the re-issue of Personal Identification Numbers (PINs).

4.4.2 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 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 issues Authorised User IDs and Passwords (where Digital Certificates are used) to the other Authorised Users and can at any stage change a password (where Digital Certificates are used) or prevent an Authorised User from logging onto the system.

e) 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.

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

Where KeyCode is used a unique Administrator password will be issued at the time of log on to each Administrator.

4.4.3 Responsibility of the Administrator

a) To log-on to the Administrator function, it is necessary for the Administrator's 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 (and verify that all Passwords remain secure and uncompromised where Digital Certificates are used). 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.

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.

4.4.4 Administrators and KeyCode

Where KeyCode is used a unique Administrator password will be issued at the time of log on to each Administrator.

4.4.5 Password Protection

Where KeyCode is used all 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.

Where Digital Certificates are used and KeyCode is not used-

Because Passwords are the key to BOL, it is essential that they be kept safely. It is the Customer's responsibility to ensure that Passwords are not disclosed to unauthorised personnel. For more details refer to the 'Security Guidelines' available on the Customer website.

Where you share a password, PIN or other security credential with a third party service provider ("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).

4.4.6 Use of Passwords (where Digital Certificates are used)

To ensure maximum protection it is mandatory that:

a) Customers change passwords frequently (regular prompts will be given by the system)

b) Passwords must be 8 characters long.

c) The Payments Password (Digital Certificate Password) must be between 8-15 characters and must be made up of alpha and numeric.

d) New passwords must be different from the last six passwords used.

e) Blank spaces must not be used in passwords.

f) Authorised Users must keep passwords secret at all times.

g) Unauthorised personnel should not be able to gain access to a password.

h) Whenever an Authorised User suspects his/her password has been compromised, it should be change immediately.

i) Obvious passwords, such as those using any identifiable sequences such as names or dates of birth, are never to be used. They should be easy for the Authorised User to remember, but difficult for anyone else to guess, eavesdrop or discover quickly by trial and error.

j) Passwords are never written down unless they are stored in a secure place (such as in a signed and sealed envelope in an office safe).

k) If an Authorised User forgets his/her password he or she should ask the Administrator for a new one

l) If the Administrator's password is lost or forgotten it may take at least three working days to receive a new one from the Bank.

4.4.7 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:

4.4.7.1 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 password.

To limit exposure to fraud the Customer should:

a) Split the power to initiate a transaction from the power to authorise it, so that no one can do both.

b) Set authorisation thresholds to limit exposure. Only employees who have full security clearance to all company financial information should be allowed to authorise payments.

4.4.7.2 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.

4.4.7.3 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.

4.4.7.4 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.

4.4.7.5 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.

4.4.7.6 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@boimail.com

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

Don'ts:

a) Allow unauthorised personnel access to BOL under your credentials.

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. 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.

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.

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) SEPA Bulk files can be post dated for up to 60 days, allowing you to set-up Direct Debit and Credit transfers, wages prior to going on business trips or holidays. These can be edited or cancelled up to two days prior to the payment date, subject to cut-off times.

c) 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.

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

essential maintenance to BOL. Other than in exceptional cases, this will be restricted to the hours of 19.00 hrs to 07:00 hrs.

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.

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.
6. The About SEPA Link on the Bank of Ireland website (www.boi.ie/sepa)

Section 3. Technical specifications

Operating Systems

Windows 7, 8, 8.1 & 10

MAC OS X 10.7 (or higher)

**Java Latest version from www.java.com

Browsers

Optimised for:

Internet Explorer Versions 9, 10, & 11

Mozilla Firefox 16+, Safari 7+

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 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 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 Digipass Devices

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.

4.3.2 Registration

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.

4.3.3 Logon

Access to BOL Payments Plus is by way of a one-time password which is generated by the Digipass and 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 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) which is generated on the Digipass.

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 transmissi on 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 full responsibility for transmission and authorisation of payment files and as such should be available to and of appropriate level of authority with the organisation to discharge these responsibilities. We recommended the appointment of two Administrator(s)

d. User Logon credentials and the Digipass and Digipass PIN should be held with the utmost care and security.

e. Loss of the User Logon and/or Digipass or Digipass PIN 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

(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.

4.4.3 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 (Digipass)

As the unlock code is the key to BOL Payments Plus, it is essential that it be 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.

Where you share a password, PIN or other security credential with a third party service provider ("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).

4.4.5 Use of Passwords

The administrator creates the initial Digipasseates the initial Digipass unlock code (5-digits). unlock code (5-digits).

a. The Bank will not have knowledge of this unlock code and therefore the customer has full responsibility.

b. The Digipass unlock code will revoke after 9 unsuccessful logon attempts.

c. The Bank cannot reset the Digipass PIN and in this instance. In the event of a lost of stolen Digipass or PIN, a new device must be ordered by calling the BOL Payments Plus Customer Support Unit and it may take a number of days before a replacement t device is received. 4.4.6 Reducing the Risk of Fraud

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 ownership of a Digipass 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. 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 understand 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 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.

Don'ts:

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

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.

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.

SEPA Credit Transfer Conversion Service:

Standard 18 File Specification – BOL Import

BOI Standard 18 File Specification – Contents

Bank of Ireland
For small steps, for big steps, for life

BOI Standard 18 File Specification – Introduction

SEPA, which stands for the 'Single Euro Payments Area', is an EU-driven regulation, and your business must be SEPA compliant for all non-urgent euro credit transfers (SEPA payments) by the 1st February 2014 deadline. Further background information is available on our website: http://bankofireland.com/SEPA

The key change that SEPA introduced for **credit transfer** files (direct credit/direct pay, via WINBITS, Business On Line and Connect:Direct) is that the current IRECC STD-18 file formats will be replaced by a new SEPA file format, SEPA XML, and the beneficiary account identifiers will change from Sort Code & Account Number to BIC & IBAN.

Bank of Ireland's approach to supporting our customers become SEPA compliant for credit transfers is to provide a file conversion service.

Our file conversion service will convert your domestic STD-18 files, on receipt by Bank of Ireland, to the new SEPA XML format, and we can then process your payment file as SEPA payments.

To process your existing payment files under the new SEPA scheme we will be required to apply stricter data quality and data completeness checks in payment files submitted to Bank of Ireland. To this end, it is essential that you adhere to the STD-18 file specification.

Purpose of this document is:

To identify the stricter SEPA data quality and data completeness checks required for payment files submitted to Bank of Ireland SEPA CT Conversion Service.

To allow you to validate that your existing STD-18 file adheres to the specification outlined within and is correct.

Any payment request submitted which does not meet these standards will fail validation and be rejected.

Customers who need to implement changes to their STD-18 file must have implemented changes on or before 1st October 2013 in order to ensure the successful processing of payments in the SEPA environment.

Bank of Ireland
For small steps, for big steps, for life

SEPA CT Conversion Service File Data Requirements

The following table highlights the stricter SEPA data quality and data completeness checks required for payment files submitted to Bank of Ireland SEPA CT Conversion Service.

The changes included relate to data rather than file structure.

Record - Field	Field Name	Position	Data Requirement
User Header Label - 3	Processing Date	5-10	The date populated in the processing date field must be the date that the customer wants the beneficiary to receive value for the transactions. 3 day cycle will no longer be available under SEPA. The file must be received by BOI before the agreed cut off time (15:30), at least 1 business day in advance of the processing date in the file
Data Record - A	NSC of the branch to be credited	1-6	The following NSC's are not reachable under SEPA, therefore payment will be rejected if present in file ► 90-89-91 (FA) ► 90-89-32 (PTSB)
Data Record - E and F	Originating Sort Code Originating Account No	18-23 24-31	The NSC and account number of the contra record must be populated in this field
Data Record - I	Users Name	47-64	Payers name must be populated in this field Payment will be rejected if not populated with 'Payers Name'
Data Record - J	Users Reference Number	65-82	The payers reference will travel with the payment to the beneficiary - If payers reference is not populated "Not Provided" will be auto populated by the conversion service and sent to the beneficiary with the payment ► BOI strongly advises file submitters to populate this field with a meaningful reference to uniquely identify the payment – this will help in identification of rejections and correspondence with the bank
Data Record - K	Destination A/C Name	83-100	Destination account field must be populated with the beneficiary name This is mandatory and payment will be rejected if this field is not populated with a reasonable name
ALL	ALL FIELDS	ALL	Please see the allowed SEPA character set detailed under Section 7

Customers who need to implement changes to their STD-18 file must have implemented changes on or before 1st October 2013 in order to ensure the successful processing of payments in the SEPA environment.

Bank of Ireland

For small steps, for big steps, for life

File Specification

1. Volume Header Label (80 Characters)

Field	Name	Length in Characters	Character Positions	Field Content and Validity Check	Field Content for SEPA Conversion
1.	Label Identifier	3	1-3	Must be 'VOL'	
2.	Label Number	1	4	Must be '1' (numeric)	
3.	Volume Serial Number	6	5-10	Can be any six characters Blanks are not permitted Must not be all zeros	
4.	Filler	31	11-41	Should be blank space filled	
5.	Owner Identification	6	42-47	Must be an authorised I.D. number (issued by BOI)	
6.	Filler	33	48-80	Should be blank space filled	

2. File Header Label (80 Characters)

Field	Name	Length in Characters	Character Positions	Field Content and Validity Check	Field Content for SEPA Conversion
1.	Label Identifier	3	1-3	Must be 'HDR'	
2.	Label Number	1	4	Must be' 1'(numeric)	
3.	Reserved for further standardization	1	5	Should be blank space filled	
4.	File Identifier	17	6-22	6 Must be 'A' 7-12 Must be authorised user I.D. number. Must be same as character positions 42-47 on volume header label 13 Must be 'S' 14-22 Must be blank space filled	
5.	Block Length	5	23-27	Must be five zeros	
6.	Filler	1	28	Must be blank space filled	
7.	Begin Extent	5	29-33	Must be five zeros	
8.	Filler	1	34	Must be blank space filled	
9.	End Extent	5	35-39	Must be five zeros	
10.	Record Format	1	40	Must be blank space filled or 'F'	
11.	Filler	7	41-47	Must be blank space filled	
12.	Creation Date	6	48-53	Must be in the form 'YYMMDD'. Must be less than or equal to the processing date in character positions 5-10 of the user header label	
13.	Record Length	4	54-57	Should be '0100'	
14.	Filler	5	58-62	Should be blank space filled	
15.	Record Attribute	1	63	Must be 'B'	
16.	Filler	17	64-80	Must be blank space filled	

3. User Header Label (80 Characters)

Field	Name	Length in Characters	Character Positions	Field Content and Validity Check	Field Content for SEPA Conversion
1.	Label Identifier	3	1-3	Must be 'UHL'	
2.	Label Number	1	4	Must be '1' (numeric)	
3.	Processing Date	6	5-10	Must in form 'bYYDDD*', i.e. a blank space Followed by the last two digits of the year and the julian day in the year	See note below*
4.	Filler	4	11-14	Must be zero filled	
5.	Receiver ID	2	15-16	Must be '90' for euro files. Must be '30' for all GBP files	
6.	Filler	4	17-20	Must be blank space filled	
7.	Currency Code	2	21-22	Must be '01'	
8.	Filler	6	23-28	Must be zero filled	
9.	Work Code	9	29-37	Must be in form '1bDAILYbb'	
10.	File Number	3	38-40	Must be all numeric, this must not exceed '968'	
11.	Filler	40	41-80	Must be blank space filled	

Notes

*** Field 3 – Processing Date**

For SEPA payments, the processing date entered in position 5-10 of the UHL1 record will be deemed to be the date that the customer wants the beneficiary to receive **value** for the transactions. To achieve this value, files must be submitted to BOI one business day in advance of this date before a pre-agreed cut-off time. Any files submitted after this time, with a processing date of the next day, will have the processing date rolled to the next available business day. Files can continue to be sent with future dates as is the case today but again the processing date on the file will be deemed to be the date that all Payees receive value for payments and the contra is posted to the customer account.

- Example 1; Customer sends file on Wednesday the 1st before pre-agreed cut-off, the processing date field must have a date of the 2nd if payment to the beneficiary is required on the 2nd
- Example 2; Customer sends file on Wednesday the 1st but wants payments to be made to the beneficiary for value on Friday the 3rd – again the processing date field in this case must have the 3rd

4. Data Record (100/106 Characters)

Field	Name	Length in Characters	Character Positions	Field Content and Validity Check	Field Content for SEPA Conversion
A.	Destination Sorting Code Number of bank branch to be CR/DR	6	1-6	Must be a valid sorting code number allocated in the current list	
B.	Destination Account Number to be Cr/Dr at the above bank branch	8	7-14	Must be all numeric	
C.	Type of account code	1	15	Must be zero	
D.	Transaction Code	2	16-17	Must be one of the permitted transaction codes	
E.	Originating Sorting Code Number at which user's nominated A/C is held	6	18-23	Must be sorting code number of one of the user's nominated accounts of branch	Under SEPA, this field must be the primary debit NSC
F.	Originating Account Number of user	8	24-31	Must be the account number of one of the user's nominated accounts	Under SEPA, this field must be the primary debit account number
G.	Filler	4	32-35	Must be zero filled	
H.	Amount in cents	11	36-46	Must be all numeric, but the characters must NOT all be zeros. Must be right justified and zero filled (note max amount for a single SEPA transaction is €999,999,999.00)	
I.	User's Name[1]	18	47-64	The payer's name must be present in this field	Payment will be rejected if not populated with payers name'
J.	User's Reference Number	18	65-82	Must be unique end to end payer's reference in this field. The Bank would strongly advise customers to populate this field with a unique reference that is meaningful to both themselves and the beneficiary e.g. invoice number etc	Where reference not populated the payment will be processed and bank will populate this field with - 'Not Provided'
K.	Destination A/C Name	18	83-100	Must be the beneficiaries name i.e. the name of the account being credited This field should always be completed	Payment will be rejected if not populated

5. Contra Records (100/106 Characters)

Field	Name	Length in Characters	Character Positions	Field Content and Validity Check	Field Content for SEPA Conversion
A.	Sorting Code Number of the bank branch at which the nominated account of the user is held and which this record is to be directed	6	1-6	Must be sorting code number of one of user's nominated accounts Must be all numeric	
B.	Account Number of the user's nominated accounts at the above branch	8	7-14	Must be the account number of one of the user's nominated accounts at the above branch Must be all numeric	
C.	Type of account code	1	15	Must be zero	
D.	Transaction Code	2	16-17	Must be '17' or '99'	
E.	Sorting Code Number of the bank branch at which the nominated at which the account of the user is held and to which this record is to be directed	6	18-23	Must be same as field A above	
F.	Account Number of the user's nominated account at the above account	8	24-31	Must be the same as field B above	
G.	Filler	4	32-35	Must be zero filled	
H.	Amount in cents unsigned	11	36-46	Must be all numeric, but the characters must NOT all be zeros Must be right justified and zero filled	
I.	User's Narrative	18	47-64	May contain alpha-numeric narrative of the user's choice	
J.	Contra Reference	18	65-82	Must be 'CONTRA' followed by twelve blank spaces	
K.	Name of account to which this record is to be directed	18	83-100	Should be equal to the name of the nominated account in fields E and F Must be left justified and blank space filled	

6. User Trailer Label (80 Characters)

Field	Name	Length in Characters	Character Positions	Field Content and Validity Check	Field Content for SEPA Conversion
1.	Label Identifier	3	1-3	Must be 'UTL'	
2.	Label Number	1	4	Must be '1' (numeric)	
3.	Monetary Total of Debit Records	13	5-17	Must contain the monetary total (in cents unsigned, right justified and zero filled) of the debit records, including credit contra	
4.	Monetary Total of Credit Records	13	18-30	Must contain the monetary total (in cents, unsigned right justified and zero filled) of the credit records, including debit contra	
5.	Count of Debit Records	7	31-37	Must contain the count (right justified and zero filled) of debit records, including credit contras	
6.	Count of Credit Records	7	38-44	Must contain the count (right justified and zero filled) of credit records including debit contras	
7.	Filler	36	45-80	Must be blank space filled	

Additional SEPA Notes:

1. SEPA will only permit National Sort Codes reachable on the IPSO Codex database. If the NSC is listed as SEPA non reachable then payments made to these NSC's will be rejected.
2. PTSB (90-89-32) and First Active (90-89-91), will not allow SEPA payments to these NSC's. Customers must ensure that no payments are sent to Bank of Ireland with these codes, it is the customers responsibility to confirm the new NSC's and account numbers for these NSC's with their payees – failure to do so will result in payments being rejected.

Bank of Ireland
For small steps, for big steps, for life


Bank of Ireland
For small steps, for big steps, for life

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

37-1436R (01/18)