# 365 Phone and Digital Banking

## Terms and Conditions

**Effective from 08 February 2024**

Bank of Ireland

These terms and conditions apply to the Services and tell you how they work. When you use a Service, you accept these terms and conditions. You have accessed the Services by following our online authentication process and completing any other procedure or providing any other Security Credential we ask you.

# What's in this brochure

## 1.0 Definitions of Terms used in this Document

Some explanations of common terms used throughout these terms and conditions:

1.1 **"365 online"** means our internet banking service accessed via a web browser.

1.2 **"365 phone"** means our telephone banking service.

1.3 **"365 PIN"** means a personal identification number you can use, together with any other Security Credentials we may ask for, to access the Services.

1.4 **"Account"** means an account with us in respect of which we provide the Services.

1.5 **"Accountholder"** means the person in whose name the Account is held.

1.6 **"Account Information Service Provider"** or **"AISP"** means a Third Party Provider that provides a service to allow you to see information in one place about payment accounts you hold with payment service providers for example your Accounts which are Online Payment Accounts.

1.7 **"Activation Code"** means a unique one time activation code which we give you and you will need for your Mobile Device to become a Registered Device.

1.8 **"Banking Day"** means any day on which we are open for business in the Republic of Ireland other than a Saturday, Sunday or bank holiday; and **"non- Banking Day"** means any other day.

1.9 **"Bank of Ireland App"** means any of our applications that can be downloaded from the relevant App store and which allow access to Bank of Ireland Mobile Banking.

1.10 **"Bank of Ireland Mobile Banking"** means our online system that allows you to access and use some of our Services using a Bank of Ireland App on your Mobile Device, and which includes Pay to Mobile. Any reference herein to Bank of Ireland Mobile Banking shall be deemed to also refer to Pay to Mobile where the reference so requires.

1.11 **"BIC"** means the Bank Identifier Code used to identify the bank internationally. It is also known as the SWIFT Address.

1.12 **"Card Based Payment Instrument Issuer"** or **"CBPII"** means a Third Party Provider that requests us to confirm if money is available in your Online Payment Accounts to fund a payment you would make using a card.

1.13 **"Cardholder"** means a person to whom we issue a credit card or debit card (for business accounts) at the request of the Accountholder.

1.14 **"Consumer"** means a natural person who is acting for purposes other than his trade, business or profession.

1.15 **"Cut-Off Time"** means the latest time in any Banking Day we can process an Instruction on that Banking Day.

1.16 **"Day of Access"** means the day you or someone else on your behalf (such as a TPP) use our Services.

1.17 **"Designated Account"** means an account you designate for receiving funds transferred from your Account. The

Designated Account can be in your name or in another person's name. It cannot be an account we tell you is excluded. Before you can make a payment to a Designated Account, you must register it using the Security Credentials we ask for.

1.18 **"Digital Banking"** (a) means our present and future online banking services which can be accessed through 365 online, Bank of Ireland Mobile Banking; and services available on bankofireland.com (b) includes a reference to 365 online and/or Bank of Ireland Mobile Banking and/or bankofireland.com where that makes sense.

1.19 **"Digital Card"** means a digital or electronic version of a credit card or a debit card which may be registered in a Digital Wallet on a compatible computer or device.

1.20 **"Digital Security Key"** has the meaning given to it in Section 5.4.

1.21 **"Digital Wallet"** means an electronic payment service that allows you to store a Digital Card on a computer or device and make payments using that Digital Card. Digital Wallets may be operated by third party Digital Wallet providers and are available on supported devices.

1.22 **"eStatement"** means any document or statement provided or made available in electronic form.

1.23 **"Future Dated Payment"** means a payment scheduled to go through on a future date (see Clause 4.7).

1.24 **"General Terms"** means clauses 1 to 21 inclusive.

1.25 **"IBAN"** means an International Bank Account Number that identifies the country, branch and account number of any account.

1.26 **"Instruction"** means any instruction or consent you or anyone else on your behalf (for example a TPP) gives us to pay money into or from your Account, or to carry out another Service.

1.27 **"Microenterprise"** means an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million as defined in Article 1 and Article 2 (1) and (3) of the Annex to Recommendation 2003/361/EC as may be amended from time to time.

1.28 **"Mobile Device"** means a communications device capable of accessing the Services using the Bank of Ireland App. For example a mobile phone or a tablet.

1.29 **"Online Payment Account"** means a Payment Account which someone can access or use through Digital Banking.

1.30 **"Pay To Mobile"** means sending a payment to another of our customer's Accounts or receiving a payment from another of our customer's using a mobile phone number. Details of this service are set out at Clause 22 below.

1.31 **"Payment Account"** means an account that is of a type that we list as a payment account on bankofireland.com.

1.32 **"Payment Initiation Service Provider"** or **"PISP"** means a Third Party Provider that provides a service in which the PISP gives instructions to us on your behalf to carry out a

payment instruction on your Online Payment Accounts where payments can be made using Digital Banking.

1.33 **"Person"** means a human being, corporation, partnership or organisation.

1.34 **"Physical Security Key"** is a small hand held physical device that can generate security codes for use in Digital Banking and be used by you as a Security Credential.

1.35 **"Policy"** means your New Ireland Assurance Company plc (NIAC) or Bank of Ireland Life (BIL) life assurance or pension policy in respect of which we provide the Services. Bank of Ireland Life is a trading name of New Ireland Assurance Company plc. New Ireland Assurance Company plc, a life assurance undertaking, is a member of Bank of Ireland Group.

1.36 **"Push Notification"** means a message we may send to your Registered Device using the Bank of Ireland Mobile Banking App. For example, Push Notifications will be used to ask you to approve or consent to certain Services or Instructions or to notify you when we provide you with important information.

1.37 **"Registered Device"** means your Mobile Device on which you have installed and registered the Bank of Ireland App by following the instructions we give you.

1.38 **"Security Credentials"** means the personalised security features we require you to use now or in future to (a) access your Account through our online, phone and mobile banking channels; and (b) to authorise transactions on your Account. Sometimes we will give you the Security Credentials; in other cases we will ask you to choose them. These are examples of Security Credentials: a personal identification number (PIN), password, one time passcode, security number or code (including those generated by a Physical Security Key ), a response to a Push Notification, your Registered Device, your fingerprint or other distinctive personal characteristics, or any combination of these features or other ones we require now or in future.

1.39 **"SEPA"** means Single Euro Payments Area, a European banking initiative which aims to create one single, integrated and standardised payments market in Europe.

1.40 **"SEPA Zone"** means the member countries of SEPA, details of which are available on Bank of Ireland website at bankofireland.com.

1.41 **"Service"** and **"Services"** include, but may not be limited to, the following, some or all of which are available via 365 phone and Digital Banking:

(a) showing you your Account balance;
(b) giving you information about your transactions;
(c) setting up and viewing Standing Orders;
(d) the cheque search facility;
(e) funds transfers and payments to Designated Accounts;
(f) a bill pay service which you can use to pay certain utility bills;
(g) requesting account statements for current, savings and loan accounts;

(h) pay to Mobile;
(i) registering and viewing other BOI accounts;
(j) viewing recent Credit Card transactions;
(k) customising Current Account transaction history on screen, for example, to list categories of transactions carried out over the previous 12 months;
(l) the services described in Clauses 20 to 22;
(m) showing you your Policy details; and
(n) such other Services as we may introduce from time to time.

You can find an up to date list of the Services available via 365 phone or Digital Banking on bankofireland.com/digitalservices.

1.42 "**these terms and conditions"** means these 365 Phone and Digital Banking Terms and Conditions. The most up to date version of these terms and conditions can be found on the Bank's website at bankofireland.com. You can also request a copy from us at any time free of charge.

1.43 **"Third Party Provider"** or **"TPP"** means any payment service provider that provides payment services to you or someone else that concerns your Accounts, for example an AISP and/or a PISP and/or a CBPII.

1.44 **"User ID"** means a unique 365 online user identification code we give you.

1.45 **"We", "Bank" "us"** and **"our"** means The Governor and Company of the Bank of Ireland, having its Head Office at Baggot Plaza, 27-33 Upper Baggot St., Dublin, D04 VX58, Ireland, and its successors, and legal or equitable transferees or assignees.

1.46 **"You"** and **"your(s)"** means (a) an Accountholder (b) a Cardholder and (c) includes you acting on your own and through anyone else you authorise to act on your behalf, for example, a TPP.

## 2.0 Accounts

2.1 You cannot use these Services unless:
(a) the Account is in your name;
(b) you are the beneficial owner of the money in the Account (this means, for example, you do not hold the money on behalf of someone else);
(c) where applicable, you have sent us a mandate for the Account and we are satisfied with it; or
(d) you are a Cardholder.

2.2 If you are a Cardholder on an Account but are not the Accountholder, your access to the Services for that Account will be limited (for example you may not be able to view balances or transactions) in accordance with the Account terms and conditions. The Accountholder is responsible for ensuring that the Cardholder complies with these terms and conditions as applicable in their capacity as a Cardholder. The Accountholder is responsible for all transactions carried out by a Cardholder using the Services and is fully liable to pay us all amounts outstanding on the Account. You will need to

use a Digital Security Key or Physical Security Key to consent to certain credit or debit card transactions.

2.3 If you select and appoint a person to use these Services:

(a) it is your sole responsibility to make such a selection and appointment and you must satisfy yourself as to the suitability and integrity of the person chosen;

(b) you agree that we shall not be liable to you or anyone else for any loss or expense as a result of us acting on the instructions of the person chosen by you to use these Services and that we can deal with that person as if he or she were you for the purposes of these terms and conditions;

(c) any change in the identity of the person authorised to use these Services must be notified to us in writing by completing the relevant form and providing it to us. The relevant forms are available by calling into any branch. Such notification will be treated as effective by us from the time of receipt;

(d) you authorise us to (but we do not have to) suspend transactions on the Account where in our sole discretion we reasonably believe we have (i) unclear authority from you or the person authorised to use the Services on your behalf or (ii) contradictory instructions in relation to the operation of the Services or the Account from two or more of the Directors, Secretary, partners, officials or persons whom we believe to be in a position of authority and we are authorised to maintain this suspension until you give a new and clear authority in the form of an Amendment Form for Existing Accounts or in another form acceptable to us. This Clause 2.3(d) is an exception to Clause 2.3(c); and

(e) some of the Services forming part of 365 Phone and/or Digital Banking may not be available to you, for a valid reason, as we may advise you from time to time. Here are examples of valid reasons:

- to better comply with a law, regulation or other legal duty;
- to reflect a change in the law, code of practice, or a decision, recommendation by a court, ombudsman or regulator;
- to improve the services we provide customers;
- to remove (or change) a service if continuing it (or not changing it) is not cost effective or sustainable or does not make a reasonable profit or provide a reasonable return on investment or equity;
- to reflect changes in our business model, or the way we do business;
- to reflect changes in technology or in our systems or to maintain our systems;
- to deal with threats to the integrity of our systems;

or

for a reason that is related to any of the previous ones.

Third Party Providers (TPP).

2.4 To use the services of a TPP for your Account, you must be able to access your Online Payment Account through Digital Banking.

2.5 Where we provide your TPP access to your Online Payment Account, you can choose to allow your TPP to access relevant information; or make relevant payments from your Online Payment Account; or both. For more information on the types of information and payments a TPP can access and make please see boi.com/PSD2.

2.6 You are not obliged to use the services of a TPP for your Online Payment Account but, if you do, it is your responsibility to read the terms and conditions of the TPP. It is also your responsibility to understand exactly what information the TPP will be able to access and how it will be used by them. This should all be covered in your agreement with the TPP. A TPP should be registered with any relevant financial services regulator in order to provide payment services to you.

2.7 A TPP may look for access to your Online Payment Account, for example, to provide payment or account information services to you. However, we will only allow such access where you have permitted us to allow that.

2.8 It is the responsibility of the TPP to ensure any information it holds about you or your Online Payment Account is secure.

2.9 About PISPs. If we receive an instruction from a PISP to initiate a payment on your Online Payment Account, we will treat this as an instruction from you.

2.10 You can instruct a PISP to initiate a payment on your Online Payment Account by following their procedures (make sure they give them to you). If you do this, you must authorise us to make the payment by using our online verification processes and your Security Credentials. Once you have authorised us in that way to make the payment initiated by the PISP we will treat the payment as though you asked us to make it yourself.

2.11 Once you have authorised us to proceed with a payment initiated by a PISP it can't be amended or stopped unless you ask us to amend or stop it before the relevant Cut-Off time.

2.12 About AISPs. If we receive an instruction from an AISP to access information about your Online Payment Account, we will treat this as an instruction from you.

2.13 You can instruct an AISP to access and hold details of your Online Payment Account by following their procedures (make sure they give them to you). If you do this, you must authorise us to share the information with the AISP by using our online verification processes and your Security Credentials. Once you have done this, the AISP can make any number of requests for access to your Online Payment Account for up to 180 days and we will obey those requests (unless we have duly evidenced reasons relating to unauthorised or fraudulent access to your Online Payment Account, in which case we may (but are not obliged to) request that you authorise us again

(in the way set out in this clause) before we share information with the AISP). Once each 180 day period passes, you need to authorise us again (in the way set out in this clause) if you wish us to continue to share information on your Online Payment Account with your AISP.

2.14 About CBPIIs. If we receive an instruction from an CBPII to find out whether money is available in your Online Payment Account to meet a card payment, we will treat this as an instruction from you.

2.15 Where we provide a CBPII access to an Online Payment Account, you can instruct a CBPII to access your account by following their procedures (make sure they give them to you). If you do this, you must authorise us to share the information with the CBPII by using our online verification processes and your Security Credentials. Once you have done this you authorise us to answer a CBPPII request to find out whether money is available in your Online Payment Account to meet a card payment. Once you have authorised us to share such information with the CBPII, the CBPII can make any number of requests for that information (and we will answer them) until you contact the CPBII to cancel your permission to allow them make such requests (you may need to follow their procedures to cancel your permission).

2.16 TPPs when you have a joint account. If the Online Payment Account is in the name of two or more of you, one of you can instruct a TPP to access your Online Payment Account details or initiate a payment on your Online Payment Account by using the TPP's procedures and ours. If we receive a request from a TPP to access your Online Payment Account details or initiate a payment, we respond to it as if all or both of you had have made the request or asked the TPP to make it on behalf of each of you.

2.17 At any time you wish you can:

(a) cancel any service that a TPP provides you that concerns your Online Payment Account; or

(b) any consent or permission you give a TPP that concerns your Online Payment Account. You may have to follow the TPP's procedure to make sure they cancel their service or stop acting on your consent or permission.

2.18 If you send your TPP a cancellation when we are processing an instruction from them or to get access to information about your Online Payment Account, it may be too late for us to cancel the instruction; and, if so, you permit us to obey it.

2.19 If you permit a TPP to access your Online Payment Account and/or to initiate a payment transaction (for example, a payment from your Online Payment Account):

(a) the TPP will have access to your Online Payment Account(s); and

(b) we are not responsible for anything the TPP does.

2.20 We may refuse to process an instruction from a TPP where we know, or have reasonable grounds to suspect:

(a) that you have not authorised a TPP to give the instruction; or

(b) that the instruction from the TPP may be fraudulent or given by mistake.

If we can identify the TPP, we will contact you as soon as we reasonably can in a way we choose, unless the law prevents us from doing so or we reasonably believe it would compromise our security measures.

2.21 We record the instruction you and any TPP give us. If there is a dispute between you and us or you and a TPP concerning any Online Payment Account, we may give our records as evidence in any way that the law allows for.

## 3.0 Policies

Remember – if you need a conclusive statement, please contact NIAC/BIL.

3.1 You can only register a Policy for viewing if the Policy is in your name or you are the sole member of a pension scheme where trustee consent has been provided.

3.2 If your Policy is held in the name of two or more persons, any of the Policy holders can use the Services and as a Policy holder you will have access to information on the other Policy holders and lives assured under the Policy.

3.3 Subject to 3.4 below, any Policy value or benefits displayed will be the value or benefits at close of business on the Banking Day before the Day of Access.

3.4 While we make every reasonable effort to ensure the information we give you about your Policy is accurate and complete, the information is not conclusive evidence of the state of your Policy. If you need a conclusive statement, please contact New Ireland Assurance Company PLC (NIAC) / Bank of Ireland Life (BIL). It is important you understand that any Policy details provided are indicative only, details provided may not include a full list of all benefits available under your Policy where benefits are displayed and the details provided do not confer any rights.

3.5 If you rely (or someone else relies) on information regarding your Policy accessed through Digital Banking and you have not asked NIAC / BIL for a conclusive statement, neither we nor NIAC / BIL will compensate you or anyone else for any loss or expense which occurs as a result of any relying on the information displayed through Digital Banking where it is different from what a conclusive statement would show.

3.6 You can only view your Policy details and, other than an Instruction to display a Policy, you cannot issue an Instruction to us in connection with your Policy.

3.7 If you wish to issue an Instruction, request a change be made, have any queries, wish to make a complaint concerning your Policy or require up to date and detailed information on your Policy, you should contact NIAC / BIL directly and not us.

## 4.0 SEPA Credit Transfers

We assume any registration or Instruction comes from you where the Services have been accessed using Security Credentials.

4.1 A SEPA Credit transfer is a payment of euro by you from your Account to a Designated Account within the SEPA Zone. It includes the payment of some bills.

4.2 We let you know how to register for our SEPA Credit transfer services. We can change the way you register for these services at any time.

4.3 We keep a record when you register to make SEPA Credit transfers and when you instruct us about this type of payment. We may give our records as evidence of your registration or Instruction in any way that the law allows for. We can assume any registration or Instruction comes from you where the Services have been accessed using Security Credentials, whether you use them or, someone else uses them where you have allowed them to do that, despite the rules in these terms and conditions which tell you not to share your Security Credentials.

4.4 You cannot use the SEPA Credit transfer service to transfer money from any loan or credit card account you have with us or one of our subsidiaries.

4.5 If you use the SEPA Credit transfer service to pay money into a loan account or credit card account you have with us, you agree that you must contact us to establish the correct balance on that Account. You cannot rely on your own calculations.

4.6 Maximum transaction and daily limits apply to the amount you can pay from your Account in any Banking Day using our SEPA Credit transfer service. We can change these limits at any time. Details of the current limits are available when you use the service. We may allow you to set a lower limit than the maximum limit from time to time by following the procedure we specify.

4.7 If you instruct us to carry out a SEPA Credit transfer on a future date, it is a "Future Dated Payment". We will process any Future Dated Payments on the date you give us. If it is not a Banking Day, we will process it on the next Banking Day. If you instruct us to make two or more Future Dated Payments for the same future date, we will process them in the same order in which you gave us the payment instructions. If, for any reason, we are unable to process a Future Dated SEPA Credit transfer, we will notify you within the Payments Pending section.

4.8 We accept payment instructions for SEPA Credit transfers at any time. If you give us a payment instruction to pay money from your Account, we treat the Instruction as given on the Banking Day ("D") on which we actually get it, so long as it is received by us before the Cut-Off Time for SEPA Credit transfers. Details of the relevant Cut-Off Time are available on bankofireland.com and on 365 online. If we receive it after

this Cut-Off Time it will be treated as received by us on the next Banking Day. We will ensure the payee's bank is paid within one Banking Day of D.

4.9 The financial institution where the Designated Account is held controls payment into that account. We are not responsible for that.

4.10 If you give us a payment instruction to pay money to a Designated Account held by us, we pay it on the Banking Day we get your payment instruction.

## 5.0 Security and Authentication

Remember to keep your Security Credentials safe and if you think they are lost or stolen tell us straight away.

5.1 We give you a 365 PIN number which is unique to you (the "365 PIN"). You may need to use it whenever you use a Service.

5.2 We may also give you a unique 365 online user identification code ("User ID"). If we ask you for this code, you must give it to us.

5.3 As part of Digital Banking in addition to the items in 5.1. and 5.2 we provide you with Security Credentials which you can use to access your Accounts and Services and to make payments through Digital Banking.

5.4 Digital Security Key

If you use the Digital Security Key the following terms apply:

(a) When you install the Bank of Ireland App you will be required to register your Mobile Device with us. We will then ask you to follow instructions (which may include entering an Activation Code we will send you) to pair your Mobile Device with your Digital Banking profile. Your Mobile Device will then be a Registered Device and will become your Digital Security Key.

(b) You can have more than one Registered Device on your Digital Banking profile.

(c) You can register the same Registered Device with multiple Digital Banking profiles.

(d) Your Registered Device is a Security Credential once you have paired it with your Digital Banking profile by following the instructions we give you.

(e) To use the Bank of Ireland App and 365 online you must have Push Notifications enabled on your Registered Device. We may send you a Push Notification to consent to certain Services or Instructions or access Digital Banking.

(f) If you receive a Push Notification asking you to confirm a transaction that you have not initiated, you must tell us straight away. Phone us at 0818 365 365/+353 1 404 4000. You may also contact us free of charge on the Freephone number listed on our website bankofireland.com.

5.5 Physical Security Key

If you use a Physical Security Key the following terms apply:

(a) If you do not have a Registered Device, you may need a Physical Security Key to access Digital Banking and to avail of Services.

(b) When you get your Physical Security Key you will need to activate it and create a PIN which you will need every time you use the Physical Security Key. You can generate security codes for use in Digital Banking using your Physical Security Key.

(c) Once activated, your Physical Security Key is a Security Credential.

5.6 You must keep your Physical Security Key safe and if you think or know that it is lost or stolen you must tell us straight away. Phone us at 0818 365 365/+353 1 404 4000. You may also contact us free of charge on the Freephone number listed on our website bankofireland.com.

5.7 We may ask you to answer security questions, or to use another Security Credential or a combination of Security Credentials, before allowing you use a Service.

5.8 You must keep your Security Credentials secret and safe and must never share them with anyone. You must not write down or record any of them in a way that would let someone else use any of them against your will.

5.9 If you know or suspect your Security Credentials are known by someone who should not know them or your Registered Device or Physical Security Key is lost or stolen, you must tell us straight away. Phone us at 0818 365 365/+353 1 404 4000. You may also contact us free of charge on the Freephone number listed on our website bankofireland.com.

5.10 After your initial registration we will never contact you to request all your Security Credentials and we will not ask anyone else to do so on our behalf. If you receive such a request you must not supply your Security Credentials in any circumstances, and should report such activity to us immediately.

5.11 We may use software, cookies and other technologies to help us identify you to help us detect fraudulent behaviour and patterns. We may also use those technologies to check for viruses or other harmful programmes (such as malware) on the computer or Mobile Device you use to access Digital Banking. In the event we suspect or detect any fraud or unauthorised activity on your Account, we will advise you via phone call, SMS message or email as appropriate. If we deem it necessary we may block your Account and will advise you of the block and how it may be removed.

5.12 You must maintain suitable equipment to enable you use Digital Banking services, for example, a computer with a suitable browser and up-to-date security software. Further details are available under accessibility section of bankofireland.com.

5.13 We put reasonable IT security measures in place. We cannot, however, guarantee the privacy or security of any

information that concerns you and passes over the internet. This is because of the nature of the internet. If you use Digital Banking, you acknowledge and accept these risks. For example, you acknowledge it is possible for a person to intercept or interfere with e-mails.

5.14 You use our Digital Banking channels at your own risk. Our website gives you information and nothing in it is:

(a) an offer as understood in contract law;

(b) an invitation to invest;

(c) an invitation to take investment, financial or banking services from us.

5.15 We claim copyright in the contents of our website. You cannot copy or use any of this content by any means unless we agree in writing beforehand.

## 6.0 When we Act on your Instructions

6.1 You permit us to act on any Instruction you give us, or which appears to have been given by you (including through a third party for example a TPP), whether submitted via 365 Phone or Digital Banking. Other than provided at clause 6.4, you cannot withdraw this permission.

6.2 Once an Instruction is received with the correct Security Credentials, you agree that we can act on it. You understand we do not make any more security checks. Where an Instruction relates to a payment, you give your consent to the payment by providing us with the correct Security Credentials and you agree that we can process (use) your personal data to obey your Instruction and to give you the service.

6.3 We can only act on your Instructions when we get them. You acknowledge and agree there may be a time lag between the time you or a third party (such as a TPP) instructs us online and when we get that Instruction, and we can take no responsibility where the delay is beyond our reasonable control.

6.4 You agree that all Instructions, other than Instructions for Future Dated Payments, are, subject to relevant Cut-Off Times, considered to be Instructions for immediate processing, and are considered irrevocable. Instructions for Future Dated Payments are deemed irrevocable at midnight on the Banking Day prior to the Banking Day upon which the Future Dated Payment is scheduled to be processed. You can ask us to cancel or amend any Instruction, but we may not be able to do so. We will have no liability to you in respect of any such request to cancel or amend a previously issued Instruction where we are unable to do so.

Remember to check Cut-Off times for Instructions.

6.5 If we receive an Instruction that does not have the information that we need to identify the Designated Account, for example IBAN and BIC, or Account Number and Sort Code, we may refuse to process it. We will tell you if we refuse to process

an Instruction for this reason. We will not be liable to you or anyone else if that results in any loss or expense.

6.6 We can refuse to process an Instruction if you do not have enough money in your Account (or enough unused agreed overdraft limit on your Account) to make the payment. We will not be liable to you or anyone else for any loss or expense this causes.

6.7 Sometimes we need to use the Society for Worldwide Interbank Financial Telecommunications (SWIFT) to carry out an instruction from you to make a payment. SWIFT is based in Belgium and has centres in Europe and the United States of America. Your transaction data can be stored for a time in these centres.

## 7.0 Joint and Several Liability

If you have a joint account you are both (or all) equally liable to us for anything that we are owed on the Account. One of you will be able to give us an Instruction on the Account without getting permission from the other person (or other people). We can send notices and letters to just one of you and the terms and conditions say that's enough to notify both (or all) of you.

7.1 If your Account is held in the name of two or more persons at any time, any one of you may, acting alone be able to use the Services. Each of you who want to use the Services must register and apply for your own separate 365 PIN, User ID and any other Security Credentials required.

7.2 If your Account is held jointly in the name of two or more persons at any time, each of you is jointly and severally liable under these terms and conditions and for any Instruction we get from any of you. This means we can ask all or any one of you alone to pay us any money owing to us and meet any obligation arising from these terms and conditions or any Instruction any of you give us.

7.3 Unless we have agreed that we need the consent of each joint account holder or have a legal obligation to get this consent, we can act on the Instructions of only one of you. This means any one of you can ask us to do certain things with the Account without the other account holders knowing, including closing the Account, taking all or any money out of the Account, asking for communications (including statements) to be provided electronically or on paper, applying for credit or ending services.

7.4 When we send any notice to any one of you (including any eStatement or statement or document in paper form) this will be deemed to be notice to all of you.

7.5 Unless we have a legal obligation to do so we won't ordinarily ask or enquire about the reasons for any instructions or reconfirm these instructions with any other Joint Account Holder even when there is a dispute among the Joint Account Holders.

## 8.0 Recording

8.1 We record the Instructions you give us. If there is a dispute between you and us concerning the services, we may give our records as evidence in any way that the law allows for.

## 9.0 Account Balances

If you need a conclusive balance of your Account please contact us.

9.1 We will include the following things in the Account balance that we provide on that Day of Access:

9.1.1 The amount in the Account at close of business on the Banking Day before the Day of Access; and

9.1.2 (for information only) the value of all payments in or out of your Account which are made (or where value is due to be paid) on the Day of Access.

9.2 If you are checking the balance on your business credit card Accounts, we will tell you the balance on the Account at close of business one Banking Day before the Day of Access. We may not include the things mentioned in Clause 9.1.2. This Clause 9.2 is an exception to Clause 9.1.

9.3 We make every reasonable effort to ensure the information we give you and any third party (for example a TPP) about balances is accurate, complete and up to date. However:

9.3.1 This is not always possible because for example your account balance may not reflect any debit or credit transfers made since the previous Business Day;

9.3.2 This means the information we give you is not conclusive evidence of the state of your Account (if you need a conclusive statement, please contact your branch);

9.3.3 If you rely (or someone else relies) on information on your Account accessed through Digital Banking and you have not asked your branch for a conclusive statement we will not compensate you or anyone else for any loss or expense which occurs as a result of relying on information on Digital Banking where it is different from what a conclusive statement would show.

## 10.0 Managing Direct Debits

10.1 Direct debit payments are made under the SEPA Direct Debit Scheme and all direct debit payments are processed in accordance with the relevant SEPA Direct Debit Scheme Rules.

10.2 You can manage your SEPA direct debits using the Direct Debit Services. If you wish to avail of any of the available direct debit services, you must complete and submit the relevant direct debit service application form. In order to ensure that your instructions can be processed as required, you must submit any such instruction by close of business on the Banking Day before you wish the instruction to be effective.

## 11.0 Charges

11.1 We can introduce charges for the Services but, if we do, we will tell you before we introduce them. The amount of notice that we will give you will follow the laws and regulations that apply at that time.

11.2 There may be fees and charges which apply under the terms and conditions of your Account. You can find details of the relevant fees or charges in the relevant Schedule of Fees and Charges which are available from your branch or online at bankofireland.com.

11.3 Our Schedule of International Transaction Charges shows our charges for international payments, travel money and other services. It is available from your branch, or online at bankofireland.com.

11.4 We do not levy any additional charges for Bank of Ireland Mobile Banking, however your mobile network operator may charge you for using or accessing the mobile network service. Any charges applied by your mobile network operator are beyond our control and you should refer to your mobile network operator for details of such charges.

11.5 We can change our fees or charges at any time for valid reasons (as set out in Clause 12.2), but will tell you before we do and the amount of notice that we will give you will follow the laws and regulations that apply at that time.

11.6 If you use a TPP for services that concern your Account, the TPP will charge their own fees and charges for them. Anything you owe a TPP is in addition to any fees or charges you owe us on your Account(s) or for using Digital Banking.

## 12.0 Changes to these Terms and Conditions, and to the Services

12.1 We may for a valid reason:

(a) add to or change these terms and conditions at any time, for example, to meet new regulatory requirements or to enhance security.

(b) remove or change a service or add a new one at any time.

(c) introduce fees or change the fees and charges we apply.

12.2 Here are examples of valid reasons for us to make any such change:

(a) to better comply with a law, regulation or other legal duty;

(b) to reflect a change in the law, code of practice, or a decision, recommendation by a court, ombudsman or regulator;

(c) to improve the services we provide customers;

(d) to remove (or change) a service if continuing it (or not changing it) is not cost effective or sustainable or does not make a reasonable profit or provide a reasonable return on investment or equity;

(e) to reflect changes in our business model, or the way we do business;
(f) to reflect changes in technology or in our systems or to maintain our systems;
(g) to deal with threats to the integrity of our systems;
(h) for a reason that is related to any of the previous ones.

12.3 We will tell you in advance if we make any of these changes and we will give you a valid reason for any such change.

12.4 The type and amount of notice of change that we will give you will follow the laws and regulations that apply at that time, and may be in writing, by letter, electronic mail, telephone (including recorded message) or other means of communication we deem appropriate.

12.5 If we change or add to these terms and conditions, and you do not wish to accept the change, you may end this contract (there will be no charge for doing this), but first you must pay us any charges that you already owe relating to the services or these terms and conditions.

12.6 If you do not ask us to end this contract under Clause 12.5, you are deemed to accept the changes which we tell you about under Clause 12.3 on their effective date. We may change our rules concerning the Services (for example transaction limits or daily limits) at any time and without telling you in advance. We will, however, provide notice about these changes, in accordance with any applicable laws.

## 13.0 Our Responsibilities

13.1 If we make a mistake when we carry out an Instruction, we will correct that mistake. If necessary, we will pay money into your Account and correct our records of your Account. The amount we pay will ensure that your Account is restored to the way it would have been if the Instruction had not been carried out.

13.2 13.2 Sometimes, we may not be able to provide you or third party (such as a TPP) with a Service because of circumstances beyond our reasonable control, for example:
(a) a natural event such as adverse weather, an earthquake, a solar storm, flooding;
(b) war or civil disturbance ;
(c) a health event including a pandemic;
(d) strikes and industrial action;
(e) electricity failure, surges or fluctuation;
(f) failure of telephones, telephone systems, email, the internet, or of other electronic equipment (including software and networks).

13.3 Sometimes, the Services may not be available or may not work properly despite our reasonable efforts to maintain them. This may be due to a fault or malfunction of a system used to deliver the Services or due to general maintenance requirements.

13.4 We are not liable to you or anyone else for any loss or expense caused if the Services are not available or are not working

properly for any of the reasons outlined in Clause 13.2. We are not liable to you or anyone else for any loss or expense caused if we need to suspend the Services for a temporary and reasonable period to rectify any of the issues outlined in Clause 13.3.

13.5 We will not be responsible for any losses caused if:

(a) we make a payment in accordance with an Instruction and that Instruction contained an incorrect IBAN or BIC, or account number or sort code, or equivalent account details supplied by you or a third party (such as a TPP); or

(b) if we can show that a payment was made by us and received by the payee's bank within the time set out in these terms and conditions; or

(c) the payment is not possible due to a regulatory or other legal reason.

You may need to use a BIC and IBAN to give us Instructions. You need to make sure these are sent to us correctly because you might lose money if not.

13.6 We will make every reasonable effort to get back any money involved in the transaction, but we may charge you for any reasonable costs that we have to pay.

13.7 We may provide you with alert services. If we do, the details provided to you may change before and after you receive them. We're not responsible for any loss, cost or charge you incur if alert services are unavailable for any reason.

## 14.0 Your Responsibilities

You must tell us as soon as possible about an unauthorised transaction or loss or misuse of a Security Credential to help limit any loss to you.

14.1 If an unauthorised transaction occurs on your Account, you must tell us as soon as possible, but no later than 13 months after the date of the transaction. To report an unauthorised transaction, you may contact us free of charge via the Freephone number listed on our website bankofireland.com.

14.2 If an unauthorised transaction is made from your Account, we will refund your Account and (if necessary) will correct our records of your Account. It shall be the responsibility of Customers who are not Consumers or Microenterprises to demonstrate to the satisfaction of the Bank that any such transaction was actually unauthorised or incorrectly executed. The amount we pay will ensure that your Account is restored to the way it would have been if the unauthorised transaction had not happened.

14.3 Despite Clause 14.2:

(a) You will be liable for the full amount of the unauthorised transaction if it was made because you

have acted fraudulently or because you intentionally or with gross negligence breach these terms and conditions.

(b) If any unauthorised payments came about because a Security Credential (for example a 365 PIN, Physical Security Key or a Registered Device) was lost, stolen or misused, the maximum you will have to pay if you are not a Consumer or Microenterprise is €50, once you had reported the loss, theft or misuse to us without undue delay. You must take all reasonable steps to prevent loss, theft or fraudulent misuse of your Security Credentials. If you are a Consumer or Microenterprise and the loss, theft or misuse of any security credential was not detectable to you then you will have no liability. If you are not a Consumer or Microenterprise your liability is unlimited.

14.4 You agree to cooperate with us and give us information we ask for if you have a complaint about your Account and we suspect that a TPP may be responsible for it, for example, because we suspect it is the TPP's fault that an instruction was not carried out or was carried out wrongly or too late.

## 15.0 Reading this Document

15.1 Each of these terms and conditions is separate from the others. If any of them is illegal or cannot be enforced, the rest will remain in full force and effect.

15.2 If we do not enforce the rights we have under these terms and conditions or we delay enforcing them, we may still enforce those rights in the future. This applies even if we did not enforce or delayed enforcing those rights on many occasions.

15.3 In these terms and conditions we sometimes give an example of something covered by a clause or definition. We do this to assist you. The scope of these terms and conditions is not limited to these examples.

15.4 Headings and summaries in boxes used in these terms and conditions are there to assist you and do not form part of the legal agreement between you and us so they do not affect or limit the meaning of any of these terms and conditions.

15.5 A reference to the singular includes a reference to the plural and vice versa, where this makes sense. A reference to any gender includes all genders.

15.6 Any reference to law in these terms and conditions should be read to reflect later changes in the law.

15.7 Any reference to "write", "writing", "written", any other form of the verb to write (or to something that can be read) includes the following: (a) an electronic or digital instruction, signature or receipt from you where we offer you the service to make those things available electronically or digitally; and (b) any email, SMS (text message to a mobile phone), pop up on the Bank of Ireland app, by facsimile or other electronic

communication where you have given us contact details for any such means of communication.

15.8 This clause only applies to these terms and conditions if you entered them on or after 29 November 2022 and where you are a consumer under the Consumer Rights Act 2022. Nothing in these terms and conditions (a) takes away from any statutory liability (legal duty) we have to you under Part 4 of the Consumer Rights Act 2022 (our "Part 4 Liabilities") or (b) excludes or restricts any of our Part 4 Liabilities. Nothing in these terms and conditions is to be interpreted to exclude or restrict any of our Part 4 Liabilities. Here are examples of our Part 4 Liabilities: our duty to supply a service in conformity with a contract under which we supply a service to you which includes meeting the tests for subjective and objective conformity set out in Part 4 of the Act; our duty to you under any implied term that Part 4 makes part of our contract with you to supply a service; our duty to charge a reasonable price for a service where a contract between you and us does not set one out.

15.9 Any reference in these terms and conditions to us being liable to you or anyone else includes any liability for loss, expense or damage to property or reputation.

## 16.0 Making a Complaint

16.1 We're committed to providing you with excellent service at all times and hope we do not give you grounds to complain. However, if you wish to make a complaint you may do so in a number of ways. You can call or write to us, avail of our online complaints form, and advise our branch teams (bankofireland.com/help-centre/customer-complaints-process provides further details about these channels and our complaints process).

16.2 If we cannot resolve your complaint within five working days, we will respond to your complaint in writing or if we hold an email address or mobile contact details for you, you agree we may respond by email or another durable medium.

16.3 If you are not satisfied with our response you can refer the matter to the Financial Services and Pensions Ombudsman by writing to them at:
The Financial Services and Pensions Ombudsman,
Lincoln House, Lincoln Place, Dublin 2, D02 VH29.
You can find more information on how to access their resolution process by visiting their website at (fspo.ie)

## 17.0 Ending this Agreement

17.1 You may ask us in writing to end this agreement at any time. If you do, these terms and conditions will come to an end once you have paid everything you owe us in relation to the Services, and these terms and conditions.

17.2 We may end this agreement and stop a Service or Services by giving you two months' notice.

17.3 We may end this agreement immediately, stop the Services or block any payments if:

(a) you die;

(b) you are declared bankrupt or insolvent in the Republic of Ireland or anywhere else;

(c) you have failed security checks;

(d) we have reason to suspect there is unauthorised or fraudulent activity on your Account, even where we think you are innocent;

(e) we are required to do so by law, regulation or direction from an authority we have a duty to obey;

(f) you have breached these terms and conditions in such a way that we know or reasonably believe it is appropriate (in your interest or ours) to close or block your account immediately;

(g) you have breached the terms and conditions of any of your Bank of Ireland accounts in such a way that we know or reasonably believe it is appropriate (in your interest or ours) to close or block your account immediately.

17.4 We do not have to notify you beforehand if we stop, restrict or block the Services for any reason listed above. We are not liable to you or anyone else if we stop or block the Services for any reason listed above. We will tell you how the stop or block on the Services can be removed (if it can be).

17.5 If you close your account(s), you may no longer be able to use the Services. If you have any queries, please contact 365 on 0818 365 365 / +353 1 404 4000.

## 18.0 Law and Language

18.1 These terms and conditions and any matter arising from the services are governed by the laws of the Republic of Ireland. This will be so even if a court or tribunal outside the Republic of Ireland deals with them. The courts of the Republic of Ireland will have jurisdiction in connection with any dispute about or relating to these terms and conditions and the services. That jurisdiction is exclusive except where you entered these terms and conditions on or after 29 November 2022, you are a consumer under the Consumer Rights Act 2022 and you are not ordinarily resident in the Republic of Ireland.

18.2 The English language is and will be used for the purpose of interpreting these Terms and Conditions and for all communication in connection with the Account and/or the Services.

18.3 Any references to law or taxation in these terms and conditions are accurate on the print date, and should be read to reflect later changes in the law or taxation.

## 19.0 International (Non SEPA) Credit Transfers

19.1 An international (non SEPA) credit transfer is a non-euro payment by you from your Account to a Designated Account

outside the Republic of Ireland or a euro payment to a Designated Account outside the SEPA zone. We will advise you how to register for the international (non SEPA) credit transfer service. We can change the way you register for these services at any time. We will decide if a proposed Designated Account may be registered to receive international (non SEPA) transfers from you.

19.2 If we do agree to do this, you must give us the other person's IBAN and BIC (or equivalent account details), and any other information we need to register that person's account as a Designated Account.

19.3 We keep a record when you register for our international (non SEPA) credit transfer services and give us instructions relating to them. We may give our records as evidence of your registration or instruction in any way that the law allows for. You agree we can assume any registration or instruction comes from you where the Services have been accessed using Security Credentials, whether you use them or, someone else uses them where you have allowed them to do that, despite the rules in these terms and conditions which tell you not to share your Security Credentials.

19.4 Before you can make your first international (non SEPA) credit transfer to a Designated Account, we will require you to authenticate that Designated Account using your Security Credentials (or a combination of them).

19.5 You cannot use the international (non SEPA) credit transfer service to transfer money from any loan account or credit card account you have with us or one of our subsidiaries.

19.6 Maximum transaction and daily limits apply to the amount you can pay from your Account in any Banking Day using our international (non SEPA) payment service. We can change these limits at any time. Details of the current limits are available when you use the service.

19.7 We accept international (non SEPA) credit transfer instructions at any time. If you give us an international (non SEPA) credit transfer instruction to pay money from your Account, we treat the international (non SEPA) credit transfer instruction as given on the Banking Day ("D") on which we actually get it, so long as it is received by us before the Cut-Off Time for that international (non SEPA) payment. If we receive it after the Cut-Off Time it will be treated as received by us on the next Banking Day. If it is a payment in Sterling or another EEA currency (non-euro) and the payees bank is in the EEA we will ensure the payee's bank is paid within three Banking Days of D.

19.8 Other payments may take longer to process.

19.9 The financial institution where the Designated Account is held controls payment into that account. We are not responsible for that.

19.10 If we need to convert one currency to another to carry out your instruction, we will use our foreign exchange rates. We will tell you what they are when you give us your instruction.

## 20.0 Standing Orders

Setting up and cancelling standing orders are subject to Cut-Off times.

20.1 You can set up standing orders on your Current Account. We require you to register this with us first and to verify your registration using Security Credentials (or any combination of them).

20.2 We keep a record when you register for a standing order and give us instructions about it. We may give our records as evidence of any such registration or instruction in any way the law allows for. You also agree we can assume any registration or instruction comes from you where the Services have been accessed using Security Credentials, whether you use them or, someone else uses them where you have allowed them to do that, despite the rules in these terms and conditions which tell you not to share your Security Credentials.

20.3 If you wish to cancel a standing order or standing order payment, you must instruct us by close of business one Banking Day before the payment is due. If your instruction arrives later than that we won't have time to obey it before the (next) standing order is due. If that happens, we are not at fault and and we will not be liable for any loss or expense caused to you or anyone else. You can find out about our up-to-date Cut-Off times on www.bankofireland.com

## 21.0 eStatements

If your Account is registered on 365 online you will get e-statements.

21.1 Once an eligible Account is registered on 365 online, you will have access to eStatements for your Account and you will not receive paper versions of some or all documents or statements for your Account. If you request a paper copy of an eStatement we will treat this as a request for a duplicate statement and it will be managed in line with our duplicate statement process (which may include a fee). You agree that any obligation to provide you with documents or statements in these terms and conditions or any other terms and conditions agreed between you and us, are satisfied when we provide you with the relevant document or eStatement or make it available to you. Any reference to documents or statements in these terms and conditions or any other terms and conditions agreed between us, shall include a reference to documents in electronic form and eStatements as the reference so requires.

21.2 eStatements can be viewed, saved or printed in PDF format. When accessed the PDF will open in a separate window and will not time out. It is your responsibility to view the eStatement in a safe and private place and to close the window when you finish viewing the eStatement.

21.3 eStatements will be stored by us and accessible by you for a period of seven (7) years from the date they become available. You can at any time during this period download, or print and retain, a copy of the eStatement. If, however, you close an Account with us, or terminate this Agreement, the relevant eStatements will no longer be available, and you should download or print any eStatements required prior to closing any Account or terminating this Agreement.

21.4 We will send a notification by email, SMS, or other channel using the details you have provided through 365 online when a new eStatement or document is available. It is your responsibility to update your contact details if they change. You can do this through 365 online .You may be able to opt out of receiving some notifications by editing your preferences through 365 online. You will be deemed to have received an eStatement once that eStatement is available through 365 online

21.5 The provisions of Section 9 of these terms and conditions DO NOT apply to any account balance, or transaction details, provided via this eStatement service, and any account details provided via eStatement may be considered as conclusive evidence of the state of your Account.

## 22.0 Bank of Ireland Mobile Banking

The provisions of this clause 23 relate to the use of Bank of Ireland Mobile Banking and supplements the General Terms which apply to 365 online (the "General Terms"). Bank of Ireland Mobile Banking is a form of online banking, and all Services provided, and instructions processed, via Bank of Ireland Mobile Banking are provided and processed in accordance with the relevant provisions of the General Terms. If you do not use Bank of Ireland Mobile Banking, this clause does not apply to you.

22.1 In order to use Bank of Ireland Mobile Banking you must be a registered 365 online user, and must have downloaded the Bank of Ireland App from the relevant app store. You will then be able to access Bank of Ireland Mobile Banking, and the available Services, using your Security Credentials.

22.2 Because Bank of Ireland Mobile Banking gives you access to your Accounts and/or Policies, you must keep your Registered Device secure and close the Bank of Ireland App if you are not using it. The conditions relating to Security set out in your General Terms equally apply in relation to use of the Bank of Ireland App.

22.3 If you suspect that someone else knows your User ID, PIN, 365 PIN, or other Security Credentials or your Registered Device or Physical Security Key is lost or stolen you must tell us straight away. Phone us on 0818 365 365/+353 1 404 4000. You may also phone us free of charge on the Freephone number listed on our website bankofireland.com. If you fail to do so, you may be liable for any unauthorised transactions on your Account which are as a result of your Security Credentials

becoming known to someone else or your Registered Device or Physical Security Key is lost or stolen. If the loss, theft or misuse of any Security Credential was not detectable to you then you will have no liability.

22.4 We will not be liable to you for any losses you suffer or costs you incur because of circumstances beyond our reasonable control. For example:

(a) you are unable to access or use Bank of Ireland Mobile Banking for any reason;

(b) any device, hardware or software you use in connection with the Bank of Ireland App is damaged or corrupted or fails to work;

(c) you did not receive any SMS notifications or Push Notifications in a timely manner for reasons beyond our control; or

(d) there is a temporary reduced level or failure to provide any Service caused by any third party service providers including software providers and mobile operators.

22.5 You must keep all software (including antivirus software) on your Mobile Device up to date. From time to time updates to the Bank of Ireland App may be issued and depending on the update, you may not be able to use Bank of Ireland Mobile Banking until you have downloaded the latest version of the app and accepted any new terms.

22.6 Your Registered Device is your responsibility. Do not leave it unattended or accessible to unauthorised persons.

22.7 When you enable biometric data on your Registered Device (for example Face ID and Touch ID on Apple devices, and facial recognition and fingerprint on Android), it is important that you only register your own biometric data, because this is what may be used as your Security Credentials when you access your 365 online profile and Accounts.

22.8 Do not allow anyone else to use their biometric data on your Registered Device, because this may give them access to your Accounts. They may then be able to give us Instructions and/or make payments (this includes payments through your Digital Card or Bank of Ireland Mobile Banking). If someone else's biometric data is used in this way, we will consider it to be authorised by you, and you will be responsible for it.

Do not allow anyone else to use their biometric data on your Registered Device because they may be able to access your Accounts and give us Instructions.

22.9 You must delete the Bank of Ireland App from a Registered Device before you discard it.

22.10 Bank of Ireland Mobile Banking uses cookies and similar technologies ('cookies') when you register, to authenticate you when you use the Service, to help us detect fraudulent behaviour and patterns and to generally improve your experience on Bank of Ireland Mobile Banking. You can find

more information on how we use cookies in our Cookie Policy available on our website or on Bank of Ireland Mobile Banking. Certain Services, such as the ATM/branch Locator, also make use of location data sent from your Mobile Device. You will be asked to provide your consent to our processing and use of your location data if you wish to use any location-based products and services we make available. You may withdraw this consent at any time by turning off the location services settings on your Mobile Device or on the Bank of Ireland app.

22.11 We provide the Bank of Ireland App "as is" and it may not be compatible with out of date hardware and software. We grant you a non-exclusive licence to use the Bank of Ireland App solely for the purposes of using the mobile banking services. You agree that all intellectual property rights in and to the Bank of Ireland App are and remain the property of Bank of Ireland and you agree that you shall not copy, modify or adapt the Bank of Ireland App in any way. The licence granted above will expire upon termination of this Agreement by either of us. You are deemed to have accepted this licence and the terms of the licence by downloading the Bank of Ireland App to your Mobile Device.

22.12 Whilst we put reasonable IT security measures in place, we cannot guarantee the privacy or security of any information that concerns you, and passes over the internet, or via mobile networks. If you use Bank of Ireland Mobile Banking, you acknowledge and accept these risks.

22.13 We may send you information in a number of ways (as allowed by law), including by digital messages or Push Notifications through the Bank of Ireland App.

**The following sections of Clause 22 only apply to Pay to Mobile:**

22.14 Pay to Mobile allows you to make payments to or receive payments from our other customers within the Republic of Ireland only. All payment instructions received by us via Pay to Mobile are processed in accordance with the relevant provisions of the General Terms.

22.15 To send and receive Pay to Mobile payments, you must have completed the following:

(a) registration for 365 online services;
(b) registration of your mobile phone number using your Security Credentials;
(c) download of the Bank of Ireland Mobile Banking App;
(d) registration of your mobile phone number and the Account you would like to receive Pay to Mobile payments into on Digital Banking using your Security Credentials. We can change the way you register for these services at any time.

22.16 To receive Pay to Mobile payments only, you must have completed the following:

(a) registration for 365 online services;

(b) registration of your mobile phone number using your Security Credentials;

(c) registration of your mobile phone number and the Account you would like to receive Pay to Mobile payments into on Digital Banking using your Security Credentials. We can change the way you register for these services at any time.

22.17 Once you are registered to send Pay to Mobile payments you can make payments via the Bank of Ireland App by inputting the payee's mobile phone number and providing Security Credentials. By selecting a contact when using Pay to Mobile to make an instruction, you consent to the Bank of Ireland App accessing data in your address book. Before doing this, you must ensure that (i) the payee is registered to receive Pay to Mobile payments and (ii) the payee's mobile phone number you use is correct as we will not be responsible if you send money to the wrong payee. We will make every reasonable effort to get back any money involved in the transaction, but we may charge you for any reasonable costs that we have to pay. Should the payee not be registered for Pay to Mobile, you will receive a notification informing you that the payee has not registered to receive Pay to Mobile payments and no payment will be made. We will not be liable to you or anyone else for any losses you suffer or losses you incur if you attempt to send a payment to a payee who is not registered to receive Pay to Mobile payments. Please note that you cannot make Future Dated Payments using Pay to Mobile.

22.18 Once you send a Pay to Mobile payment to a registered Pay to Mobile payee, you will receive an SMS message confirming that your Pay to Mobile payment has been sent from your registered Account. The registered Pay to Mobile payee will also receive a SMS message confirming that your Pay to Mobile instruction has been made to their registered Account.

22.19 We do not charge you for sending or receiving payments through Pay to Mobile (network charges may apply for using the Bank of Ireland App). Please see Clause 11 for further details on our charges generally.

22.20 You authorise us to disclose your mobile phone number when you use Pay to Mobile or when we process your request or display this information in messages sent to any payer or payee. We will use any information you provide to us in connection with sending or receiving Pay to Mobile payments only for the purposes of administering those payments and to contact you via your registered mobile phone number in relation to your Pay to Mobile payments.

22.21 Because Pay to Mobile can be used to make payments via the Bank of Ireland Mobile Banking App, you must keep your Mobile Device secure and not logged into the Bank of Ireland Mobile Banking App.

22.22 We will not be liable to you or anyone else for any losses you suffer or costs you incur because of circumstances beyond our reasonable control. For example:

(a) you are unable to access or use Pay to Mobile;
(b) any device, hardware or software you use in connection with Pay to Mobile is damaged or corrupted or fails to work;
(c) you did not receive any SMS notifications in a timely manner for reasons beyond our control; or
(d) there is a temporary reduced level or failure to provide any Service caused by any third party service providers including software providers and mobile operators.

22.23 Minimum and maximum transaction and daily limits apply to the amount you can send or receive using Pay to Mobile. We can change these limits at any time. Details of the current limits are available when you use the Pay to Mobile service.

22.24 We keep a record when you register to make Pay to Mobile payments and when you instruct us about this type of payment. We may give our records as evidence of your registration or instruction in any way the law allows for. You agree we can assume any registration or instruction comes from you where the Services have been accessed using Security Credentials, whether you use them or, someone else uses them where you have allowed them to do that, despite the rules in these terms and conditions which tell you not to share your Security Credentials.

22.25 You cannot use the Pay to Mobile service to transfer money from any loan or credit card account you have with us or one of our subsidiaries.

## 23.0 Digital Financial Wellbeing

Tools alerts and insights are not financial advice or recommendations.

23.1 We provide a range of digital financial wellbeing services through Digital Banking. These digital financial wellbeing services include financial tools, alerts or insights based on your Account activity. These tools, alerts and insights are provided for information purposes only and do not represent financial advice or recommendations.

23.2 To provide digital financial wellbeing services, we need to monitor and analyse your Accounts. Using your Account information, we can identify transactions or activities (for example, recurring payments, low balances, upcoming bills or spending patterns) and provide you with insights or alerts to help you manage your finances. These tools, insights and alerts will be displayed to you through Digital Banking. We may also in the future, send you alerts (including using Push Notifications) to make you aware of these tools and insights.

23.3 If we send you alerts or present you with insights, we cannot guarantee that you will always receive those alerts or insights or that you will receive them in a timely manner relevant to the information for every alert or insight that is generated.

Alerts may not be sent or insights may not be presented on a "real time" basis and may instead be sent at the next scheduled delivery time and you should therefore not treat all alerts or insights as providing "real time" information in relation to your account.

23.4 The insights and alerts we may provide to you are for information purposes only based on your transaction history and do not comprise advice or recommendations. Any information that we provide through insights or alerts is designed to help you improve your digital financial wellbeing. It is not financial, professional, legal or tax advice and you should seek your own independent advice on these matters.

23.5 To be able to use digital financial wellbeing services:

(a) You must be registered for Digital Banking and use the most up-to-date security software and version of the Bank of Ireland App or website browser; and

(b) You must be a personal banking Accountholder. Digital financial wellbeing service are not currently available for business banking or corporate customers.

23.6 Digital financial wellbeing services may not be able to provide insights or alerts for all accounts or customers. More detailed information on the accounts which can be included in digital financial wellbeing services or any exclusions, are available on our website. Currently, the following are excluded from digital financial wellbeing services:

(a) The details provided to you in an insight or alert do not include in progress transactions;

(b) Additional Cardholders will not have transactions carried out using an additional card included in their insights or alerts; and

(c) Where you have accounts with us in more than one jurisdiction, insights or alerts will only be served on your primary account.

If you have multiple current accounts with us, insights or alerts will be served on your accounts on a combined basis.

37-1541R.5 (02/24)

Bank of Ireland

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