GENERAL TERMS AND CONDITIONS OF THE EASY BANKING APP SERVICE

Also known by its commercial name Hello bank! app

(Valid as from 01/07/2019)

I. **GENERAL**

The Easy Banking App service is subject to the General Terms and Conditions of BNP Paribas Fortis, whose head office is located at Montagne du Parc/Warandeberg 3, B-1000 Brussel s, Belgium, Brussels Register of Companies, VAT BE 0403.199.702, FSMA no. 25879A. In accordance with the BNP Paribas Fortis General Terms and Conditions, specific features of the Easy Banking App are outlined in these General Terms and Conditions, in the agreement or application signed by the subscriber, the terms of use for the Easy Banking App/Hello bank! app available in the application concerned (as well as at the websites below), the technical information available at (www.bnpparibasfortis.be and www.hellobank.be) and in notices of changes sent to the subscriber in accordance with the procedures that appear in Article XII below.

The Bank reserves the right to call upon subcontractors for the provision of the aforementioned service.

II. **GLOSSARY**

These General Terms and Conditions use the following terms:

- Bank: BNP Paribas Fortis SA/NV, hereinafter referred to as "the Bank" or "BNP Paribas Fortis SA/NV" acting either on its own behalf or for other entities which may or may not be part of the BNP Paribas Group, for which it acts as an intermediary, sub-contractor or partner;
- debit card: a debit card issued by BNP Paribas Fortis, under the BNP Paribas Fortis or Hello Bank trademark, and covered by the General Terms and Conditions for Easy Banking Phone and Easy Banking Web cards and services;
- CARD STOP: entity appointed by the Bank to be notified in the event of loss, theft or the risk of improper use of a card;
- Accounts held with the Bank: any account held with the Bank and accessible through the Easy Banking App service
- Aggregated accounts and aggregated information: some existing accounts held by the subscriber, and for which he is the account holder, with another financial institution, as well as the information relating to their usage. Only accounts and information added by the subscriber within the Easy Banking App service shall be deemed to be aggregated accounts and aggregated information. The list of accounts and information, as well as the financial institutions for which access to the accounts by the Bank is possible , can be viewed on our websites (www.bnpparibasfortis.be on the Easy Banking App page, and www.hellobank.be), as well as our mobile applications.
- subscriber: a natural person who uses the Easy Banking App service;
- account holder: a natural person or a legal entity holding an account, current account or savings account to which the transactions carried out via the Easy Banking App service relate;
- available account balance: amount obtained by adding the balance of the account held with the Bank to the amounts of any credit or overdraft facilities granted by the Bank in relation to the account concerned;
- mobile applications: computer applications provided by the Bank under the BNP Paribas Fortis or Hello Bank trademark for the purpose of accessing and using the Easy Banking App service;
- device: all devices that allow the holder to connect to the internet, including, in particular: smartphones and tablets;
- identification and/or signature procedures: electronic identification and/or signature techniques which are accepted as having evidentiary value as defined in Article 22.2 of the General Banking Terms and Conditions, more specifically:
  - access number and debit card number
  - recognition of the registered device and the password
  - a card reader, using the card and pin code linked to the card,
  - fingerprint and/or facial characteristics recognition matching the subscriber on the device, available on iOS and Android platforms (function supplied by the mobile device manufacturer and/or the operating system developer)
  - using the itsme Application and the itsme Code

which are provided by the Bank or accepted by it and which allow subscribers, depending on the options provided by the Bank, to identify themselves when accessing the Easy Banking App service, and to approve and/or to sign certain types of orders and/or requests that are transmitted while using it;

- access number (or customer number): the unique customer number used by the subscriber during the identification process;
- PIN: personal confidential ID number that is linked to the card and used by the subscriber during the identification process;
- password: personal confidential ID number used by the subscriber for identification purposes;
- device registration: unique secured identification of the device, kept by the Bank, which allows the device to be identified during the use of the Easy Banking App service;
- fingerprint/facial recognition: biometric characteristics of the account holder which s/he records on his/her device that supports this, to identify him/herself on this device and that the account holder can activate for use as an authentication process using the mobile app.
- itsme Services
  - itsme Application: mobile application provided by Belgian Mobile ID SA (registered office at Place Sainte Gudule 5, 1000 Brussels, BCE/KBO number: 0541.659.084). Depending on the options that the Bank provides, the itsme Application's functionalities may be used as an identification procedure as part of the procedure for accessing the Bank's digital channels and/ for approving certain orders and transactions initiated within those channels;
  - itsme Account: personal account which has to be created in advance with Belgian Mobile ID SA in order to use the itsme Application;
  - itsme Code: personal and confidential identification code created directly in the itsme Application by the user, to access and use its itsme Account.

III. **PROVISIONS FOR ACCESS TO THE EASY BANKING APP SERVICE AND THE ACCOUNTS - DELIVERY OF MEANS OF ACCESS**

III.1. **Conditions for accessing the Easy Banking App service**

Only the following people may access and use the Easy Banking App service:

- subscribers to the Easy Banking Web service aged 18 and over.

Customers can subscribe to the Easy Banking App service from the mobile application, as soon as they download it.

- subscribers to the Easy Banking Web service aged 15 and over, as subscribed to under a Welcome Pack. Subscription to the Easy Banking App service for those under 18 will be done beforehand by their legal representative(s) using the channels provided by the Bank for this purpose.

Access and use of the Easy Banking App service are only allowed in observance of Article VI.6 of these General Terms and Conditions (minimum configuration and security measures required by the device) and exclusively via mobile applications provided by the Bank, namely:

- the Easy Banking App under the BNP Paribas Fortis brand;
- the Hello bank! app for the Hello bank! brand.

Login terms and conditions can be found on our www.bnpparibasfortis.be websites, on the Easy Banking App page, and at www.hellobank.be.

This connection method is subject to change.

III.1.1 **Easy Banking App identification means**

The subscriber must use the identification procedure provided by or accepted by the Bank to identify herself or himself to the Easy Banking App or Hello bank! App as described below, and follow the on-screen instructions.

The first time a subscriber logs in, they will identify themselves using a card reader, along with the card and PIN code.

Subscribers must enter the following data: their access number and debit card number. The subscriber can choose a user name to save this data for future use of the Easy Banking App service.

Following which an electronic signature is created by pressing M1 on the card reader then following the instructions displayed on the screen.

After this first-time identification:

- some characteristics of the device on which the mobile application is installed are automatically saved;
- subscribers can activate the fingerprint and/or facial recognition function on their profile for their device, if it supports it, and to which they have sole access, by recording only their own biometric characteristics.

Thereafter, each time a subscriber logs in to the Easy Banking App service, choice can be made between:

- Identification with the Easy Banking App password: once their device has been saved, the subscriber can

subsequently log in using only the password chosen when they signed up to the Easy Banking App service. This is because the mobile application recognises the device.

- Identification using a fingerprint/facial recognition: by virtue of the options provided by the Bank depending on the mobile application used, following activation of the fingerprint or facial recognition function, subscribers can connect using (one of) their biometric characteristics that they have recorded on a device which supports this function.

- Identification with a card reader by using the card and PIN.

- Identification using the itsme Application and the itsme Code

Depending on the options provided by the Bank, any subscriber, who must be at least 18 years old, who wants to use the itsme application to identify him or herself during the procedure for accessing the Easy Banking App and Easy Banking Web services (the latter being covered by the General Terms and Conditions relating to debit cards, and the Easy Banking Phone and Easy Banking Web services) and/or for approving certain orders and transactions initiated while using these services, must:

- first register in the itsme Application by setting up his/her itsme account with Belgian Mobile ID SA, with its associated itsme Code of his/her choice, in line with the procedures and conditions defined in the agreement between the holder and Belgian Mobile ID;

- then activate his or her itsme Account within the context of Easy Banking Web or Easy Banking App services by following the instructions and information provided via the selected service.

The subscriber shall use the identification and signature procedures provided for this purpose by the Bank.

Registration of the mobile device can be deactivated at any time by the subscriber, including the legal representative of subscribers under 18, by calling the Easy Banking Centre Helpdesk (+32 2 433 41 90) for Easy Banking App mobile applications or the Hello Team (+32 2 433 41 45) for Hello bank! app mobile applications.

Subscribers can deactivate the fingerprint recognition or facial recognition function in the mobile application on their device at any time, without this affecting the other log in methods.

The Bank reserves the right to deactivate the registration of the device and thus to disable the password and fingerprint identification or facial recognition means at any time in the event of technical issues, suspicion of improper or fraudulent use, non-use of the device for more than 90 days or for any other objective security reason. Whenever device registration is deactivated, either by the Bank or at the subscriber's request, the subscriber may continue to use the Easy Banking App service by logging in using the card reader with the card and PIN code.

The holder may block its itsme Account at any time through the itsme website: www.itsme.be. He or she can then access and use the Easy Banking App service by making use of identification and signature procedures that the Bank makes available.

III.1.2 **Entering incorrect passwords, PINs and itsme Codes**

Easy Banking App can no longer be used if three incorrect passwords are typed in.

In this case, or if the subscriber has forgotten their password, the password can be changed using the mobile application accessed using a card reader with the card and PIN.

The debit card can no longer be used after three incorrect PINs are typed in in a row as part of the identification or signature means using the card reader. Subscribers who have forgotten their PIN should request the Bank to issue a new PIN.

The itsme Account will be blocked after an incorrect itsme Code has been entered three consecutive times. To unblock the itsme Account and obtain a new itsme Code, the account holder must re-register in the itsme application using the functionality provided through the Bank's channels or via itsme channels, following the instructions provided.

III.1.3 **Password, PIN and itsme code security**

The password selected by the customer, the PIN and the itsme code are strictly personal and confidential.

The Bank takes suitable measures to make sure that the password, PIN and itsme code used for the Easy Banking App service are kept secret.

III.1.4 **Invalid fingerprints/facial recognition**

After several failures to recognise the fingerprint/facial recognition, subscribers must comply with the iOS or Android platform procedures and instructions.

III.2. **Terms of access to services**

The Easy Banking App service is activated when it is used for the first time.

Once they have identified themselves as defined in Article III.1.1, they have access to the services described in Article IV below.

III.3. **Terms of access to the accounts**

Service subscribers over 18 can access the following accounts held with the Bank for financial transactions carried out by the Easy Banking App, depending on the mobile application used as specified in Article III.1 above:

- all accounts of which they are (co-)holder;

- all accounts for which the subscriber is usufructuary. In this case, the Easy Banking App subscriber is only authorised to carry out the following transactions: balance checking for these accounts and the transactions occurring in them;
- all the accounts of which they are a signatory;
- all accounts opened in the name of a person for whom they are a legal representative.

Service subscribers under 18 can access any current or savings accounts held with the Bank for which they are the holder, co-holder, agent or usufructuary.

The subscriber can also access aggregated accounts and aggregated information as set out in article IV.2 of these General Terms and Conditions.

Whenever the subscriber carries out a transaction using Easy Banking App, they can view the list of available accounts on the device screen. This list is constantly updated to take account of events that affect the status of these accounts or change the Easy Banking App subscriber's relation to these accounts.

Subscribers to the Easy Banking App service may only carry out those transactions on an account that are compatible with the scope of their authorisation to use the account in question.

IV. **DESCRIPTION AND USE OF THE SERVICE**

IV.1**. Services linked to Easy Banking App for the Bank's accounts and services**

Easy Banking App allows the subscriber:

- to connect to the Bank's computer system with a device to access certain services within the restrictions and conditions provided in these General Terms and Conditions. These services include making account enquiries, obtaining information on banking and insurance products, making transfers, purchasing and managing certain financial or other services marketed by the Bank. The list of features and transactions available via the device screen is available in the menu of the mobile application concerned.

- to contact a Bank adviser by phone, to access, subject to the limits and conditions set out in these General Terms and Conditions, for the purposes listed above and to carry out investment transactions, transmit orders and requests, obtain general financial information and personalised information and advice. The list of features and transactions available from a Bank adviser is available from the Bank.

These lists are subject to change. The Bank can add, change or cancel certain services.

Certain services may be governed by special terms and conditions. Registering for these services implies the acceptance and application of their specific terms and conditions.

In relation to the features and transactions available via the device screen:

Depending on the options provided by the Bank, the account holder may use the signature procedures made available by or accepted by the Bank to approve and/or sign certain orders and/or requests including the purchase of financial or other services marketed by the Bank. Unless a technical incident interrupts the operation, the account holder is informed immediately of the result of his or her request (acceptance, non-acceptance or review by the Bank).

In relation to the features and transactions available from a Bank adviser:

All telephone conversations are recorded by the Bank.

The Bank shall confirm to the account holder if his/her request is accepted, and will provide him/her with all the necessary information by means of a message attached to the account statements, by a simple letter or any other electronic messaging system. When the request relates to services that the Bank markets on behalf of other entities, the confirmation of acceptance of the request may, in some cases, come directly from the other entity concerned.

IV. 1.1 **Zoomit**

The Easy Banking App service allows subscribers to use the Zoomit service via the mobile application to accept a sender, access documents from this sender and manage them.

The payment, via Easy Banking App, of invoices made available as part of the Zoomit service, takes place within the amount limits set, which apply to all transfers made to a third party, under Article V below.

The Zoomit service is governed by the Zoomit service regulations, which can be found in Appendix 1 to the General Terms and Conditions for debit cards and Easy Banking Phone and Easy Banking Web services.

IV. 1.2 **Mobile payments (Bancontact)**

By virtue of the options provided by the Bank, depending on the mobile application used, the Easy Banking App service enables mobile payment transactions to be made.

A mobile payment transaction is a transaction using a card, that is, a transaction transferring funds in euros, linked to the holder's debit card, which the Bank has issued and which is governed by the general terms and conditions applicable to the Bank's debit cards.

The user accesses the functionality using the corresponding screen of the mobile application. The functionality requires a device that has a camera with autofocus.

The user follows the instructions on the screen of the mobile application to select which of the cards they hold they would like to use, and in order to complete a mobile payment transaction as payer or beneficiary. As a payer, the user can pay any individual who has a Bancontact debit

card and a mobile application with the appropriate Bancontact mobile payment functionality; they can pay any retailer offering the mobile payment option online at the point-of-sale.

The holder acting as payer irrevocably authorises the transaction through the identification and/or signature process that the Bank specifies on the corresponding screen; in so doing, they authorise the Bank to debit the amount of the mobile transaction that they have authorised from the account linked to the card selected. The transaction is regarded as received by the Bank when the mobile application confirms to the user on screen that the transaction has been successful and the amount of that transaction.

The mobile payment transaction authorised by the user as payer is completed in the timeframes and conditions - notably relating to available balance on the account to which the card selected by the user is linked - which apply to transactions using debit cards in accordance with the general terms and conditions of the Bank applicable to debit cards. The limit on the thresholds described in Article V also applies.

On the corresponding screens of the mobile payment functionality of the mobile application, the holder can view the latest mobile payment transactions for which they acted as payer or beneficiary, and the amount. All mobile payment transactions are shown in the statements of account for the account linked to the bank card with which the mobile payment transaction was completed.

IV.1.3 **Third-party payment applications**

Depending on the options offered by the Bank, the Easy Banking App service allows the subscriber to link their Bank-issued debit/credit card(s) to certain third-party payment applications pursuant to the specific provisions set out in the General Terms and Conditions applicable to the relevant card(s).

IV.2. **Services linked to Easy Banking App for aggregated accounts and aggregated information**

The subscriber may add aggregated accounts and aggregated information to the Easy Banking App and initiate transfers from these accounts in accordance with the rules set out by the financial institution with which the aggregated accounts and aggregated information are held.

Consequently, the limits and maximum amounts set out in article V below are not applicable to transfers initiated in this way.

As part of the technical procedures for adding accounts and information held with another financial institution and for the initiation of transfers on these accounts, the subscriber grants the Bank the power to accept, where applicable, in his/her name and on his/her behalf, any contractual conditions which may be applied by the financial institution with which the accounts and information are held.

The subscriber undertakes to aggregate only those accounts and information held with other financial institutions for which he or she is the sole and exclusive account holder.

The subscriber may add or delete aggregated accounts and aggregated information to/from Easy Banking App at any time.

If the subscriber has access to more than one mobile application, all the aggregated accounts and aggregated information the subscriber has added or removed from one mobile application will be automatically included or deleted from the subscriber's other mobile application(s).

The subscriber shall only have a time-limited access to the transaction history of the aggregated accounts and aggregated information.

IV.3. **Services linked to Easy Banking App for accounts held with the Bank and the aggregated accounts and aggregated information**

IV.3.1 **Carrying out transfers in euro (SEPA) using Easy Banking App**

Without prejudice to transfer orders that may be arranged through the adviser with whom the subscriber has been put in contact, transfer orders can be transferred via the Easy Banking App service, by following the on-screen instructions.

The execution of a transfer is a fully electronic transaction which works as follows:

- The transaction is presented on the screen in the menu where it can be selected by the subscriber.
- After entering the application data, these are confirmed by the subscriber. The Bank can request the subscriber to approve/ sign certain transfers to third parties electronically by using the signature procedure provided as part of the service or accepted by the Bank.
- The instruction as confirmed or signed by the Subscriber is sent and processed entirely electronically.
- The subscriber will be informed immediately – unless the transaction is interrupted due to a technical incident – of the outcome of his request (accepted or rejected).

Transfers initiated through the Easy Banking App service on aggregated accounts shall comply with the rules of the financial institution with which the aggregated account is held. The Easy Banking App service is therefore solely used as a means of transmitting the payment order.

The transfer functionality with memo date is not available for aggregated accounts.

IV.3.2**. Analysis of income and spendings**

The analysis of income and spendings enables the automatic categorisation of the subscriber's transactions made on the accounts accessible through the Easy Banking App, including aggregated accounts and aggregated information.

The various categories and sub-categories are set by default. At any time, the subscriber may:

- Change the category/sub-category automatically attributed to each of his/her transactions;
- Exclude a transaction from categorisation.
- Categorise a transaction in the event that this has not been done by default.

The subscriber may add or remove an account from the analysis of income and expenses. The subscriber may deactivatethe 'Analysis of income and expenses' functionality at any time.

If the subscriber has access to more than one mobile application, the 'Analysis of income and expenses' functionality as configured in one mobile application will be automatically included in his/her other mobile application(s).

V. LIMITS AND MAXIMUM AMOUNTS APPLICABLE TO TRANSACTIONS ON ACCOUNTS HELD WITH THE BANK

V.1. **Transfers**

Under this Article, a transfer to a third party is understood to mean any transfer to an account not accessible to the subscriber via the Easy Banking App service, i.e. an account other than those mentioned in Article III.3 of these General Terms and Conditions.

Subject to the subscriber's powers over the accounts, the following limits apply for all transfers made via Easy Banking App:

- transfers from a current account to a savings account and vice versa are limited to the available balance in the account to be debited;
- transfers to third parties made by Easy Banking App are limited:
  - For subscribers over 18:
    - Via the device screen: to a maximum of EUR 25,000 per day per account
    - Via an adviser: to a maximum of EUR 5,000 per day and EUR 10,000 per week (this limit applies to all transfers via the adviser under the terms of this agreement, via Easy Banking Phone and BNP Paribas Fortis Self Bank ATMs)
  - For subscribers under 18:
    - Via the device screen: to a maximum of EUR 625 per day and EUR 1,250 per week from a Welcome Pack
    - Via an adviser: to a maximum of EUR 625 per day and EUR 1,250 per week from a Welcome Pack (this limit applies to all transfers via the adviser under the terms of this agreement, via Easy Banking Phone and BNP Paribas Fortis ATMs).

With the exception of what is stated above in relation to transfers made via an adviser, these limits are applied separately and independently from those set for money withdrawals, payments at payment terminals and transfers as specified in the general terms and conditions applicable to debit cards and Easy Banking Phone and Easy Banking Web services.

However, the Bank reserves the right to cap this maximum amount at an amount it will set itself in the event of a risk of fraud or similar abuse.

V.2. **Mobile payments**

The following limits apply to the mobile payment transactions referred to in Article IV.1.2.:

- per transaction to an individual: minimum EUR 0.50 and maximum EUR 250;
- per transaction to a retailer: minimum EUR 0.50 and maximum EUR 500;
- per calendar day: the user may be the beneficiary of a maximum total amount of EUR 500;
- per calendar day: the user may pay one or more individuals a maximum total amount of EUR 250 using one or more of its debit cards registered in the mobile applications Easy Banking App and Hello bank! App;
- per calendar day: the user may pay one or more retailers a maximum total amount of EUR 500 using one or more of its debit cards registered in the mobile applications Easy Banking App and Hello bank! App.

These limits are applied separately and independently from those specified in the general terms and conditions applicable to the debit card used.

VI. **OBLIGATIONS AND LIABILITY OF THE HOLDER**

VI.1 **Basic obligations – Security of means of identification and signature – Security of access to the device and its use**

The subscriber must use the Easy Banking App service in accordance with the terms and conditions governing the issue and use thereof.

The subscriber must make sure that their transactions are carried out directly in the Easy Banking App service as described above. In particular, the Easy Banking App service and the identification and signature procedures (made available by the Bank as part of the Easy Banking App service) must only be accessed and used via the mobile applications provided by the Bank for this purpose.

The password, the card, the PIN and the identification and signature procedures are strictly confidential to the subscriber.

Account holders shall take all necessary precautions to ensure the security and, where appropriate, the secrecy of their password, card, PIN, including their itsme Code as well as the identification and signature procedures. In particular, they agree to memorise every password, PIN and itsme Code, not to write them down in any document, on any object, or in any electronic file and not to share them or disclose them in any way.

They also state that they shall prevent their password, PIN, itsme Code and identification and signature procedures from being accessed or obtained by any third parties.

Subscribers will also take all the necessary steps to ensure the security of access to their device, and of its use.

In particular, subscribers are required to only activate the fingerprint or facial recognition function as an identification process if they have exclusive use of the device and record only their own fingerprints / face characteristics.

It is not permitted therefore (to allow) any other person to record their fingerprints and/or face characteristics on the device, except their own.

Without prejudice to the foregoing and when the holder has activated the itsme application as identification and signature procedure as part of the Easy Banking App service, then he or she is required to respect the obligations and security measures relating to the use of the Application, the Account and the itsme Code as defined in the agreement they concluded with Belgian Mobile ID.

VI.2. **Notification of loss, theft, fraudulent use or any risk of fraudulent use of password, PIN, cards, devices and signature and identification procedures**

The subscriber shall take all necessary measures to enable him or her to recognise the following situations without delay and to carry out the required notifications.

Easy Banking App service subscribers, including the legal representative of subscribers under 18, must notify the Easy Banking Centre Helpdesk as soon as they become aware of the loss, theft or any risk of fraudulent use of their electronic identification, signature and/or device, including any fraudulent use of the fingerprint or facial recognition log in procedure.

The Easy Banking Centre Helpdesk is only accessible on certain days and at certain times. The subscriber may obtain information about the opening hours of the Easy Banking Centre Helpdesk from a branch or on the websites www.bnpparibasfortis.be and www.hellobank.be.

If the subscriber notes these facts outside the office hours of the Easy Banking Centre Helpdesk, then the notification should be made as soon as this service is accessible again or as soon as reasonably possible. If the electronic identification and signature system used to access Easy Banking App involves the use of a card and reader, subscribers, including the legal representative of subscribers under 18, must notify CARD STOP as soon as they become aware of the loss, theft or any risk of fraudulent use of the card.

CARD STOP can be reached by phone 7 days a week, 24 hours a day on 070 344 344. The phone conversation will be recorded in full by CARD STOP.

Holders who have activated the itsme Application must immediately alert Belgian Mobile ID and block their itsme Accounts as soon as they are aware of the loss, theft, use or the risk of fraudulent use of their equipment, itsme Account or itsme Code. Blocking the itsme account can be done at any time via the itsme website www.itsme.beor, during its opening hours, by calling the itsme Helpdesk phone number +32 2 657 32 13 .by following the instructions provided. All necessary information, including the opening hours of the itsme Helpdesk, is also available on the above website.

CARD STOP, the Easy Banking Centre Helpdesk, or the itsme Helpdesk as the case may be, will immediately provide the subscriber with a reference number as proof that notification has taken place.

The events notified in accordance with this Article must be reported to the police authorities of the area where the loss or theft occurred within 24 hours.

VI.3. **Notification of error or inaccuracy in account statements**

VI.3.1**. For accounts held with the Bank**

Subscribers must check the status of accounts used in the transactions carried out by the Bank through the Easy Banking App service as frequently as possible, as well as the transactions recorded on these accounts. If subscribers notice an unauthorised payment transaction in this respect, or one which has been incorrectly executed, they must act in line with the provisions under the "Payment services" heading with regard to payment transactions appearing in the Bank's General Banking Terms and Conditions.

VI.3.2. **For aggregated accounts and aggregated information**

If subscribers notice an unauthorised payment transaction from an account held with another financial institution, or one which has been incorrectly executed, through information appearing in the Easy Banking App service or through account statements of accounts issued by said financial institution, the subscriber should contact this financial institution as soon as possible. The financial institution in question shall be the sole point of contact in such a matter.

For notifications requiring action, the subscriber should refer to the contractual conditions issued by the financial institution with which the account is held.

VI.4. **Liability for fraudulent use of the Easy Banking App service, the password, PIN, the card, and signature and identification procedures**

VI.4.1. **Up until the time of notification**

Up until the time of notification as outlined in Article VI.2., subscribers are liable for the consequences of the loss, theft or fraudulent use of their device, their card or signature and identification procedures (including using fingerprint or facial recognition) up to an amount of EUR 50, unless the subscriber has acted with gross negligence or fraudulently; in this case, the maximum amount indicated does not apply. In the event of business use, the above-mentioned limit does not apply.

By way of derogation from paragraph 1, the subscriber shall not bear any loss if:

1) the loss, theft or misappropriation of a card or identification and signature procedures could not be detected by the card holder before payment, unless they acted fraudulently; or

2) the loss is due to the acts or default of an employee, agent or branch of the Bank or of an entity to which its activities have been outsourced.

VI.4.2 **After notification**

Once the notification as defined in Article VI.2 has been carried out, subscribers are no longer liable for the consequences of the loss or theft of their device, card or signature and identification procedures, unless the Bank can prove that the subscriber has acted with gross negligence or intent to defraud.

VI.4.3 **Gross negligence**

VI.4.3.1 **General**

Depending on the circumstances and without prejudice to the discretion of the court, gross negligence will arise where subscribers:

- fail to notify CARD STOP, the Bank or Belgian Mobile ID SA, that their card or device, and/or electronic identification and signature device has been lost, stolen or is at risk of fraudulent use, as soon as they become aware of the situation;
- fail to check regularly the status of accounts on which transactions have been carried out using the Easy Banking App service and the individual transactions on the accounts, if this results in a delay in the subscriber becoming aware of the fraudulent use of the signature and identification procedures and in notifying the Bank;
- fail to comply with security measures and follow precautions as set out in Articles VI.1, VI.6 and VI.7 respectively;
- fail to provide notification of the loss, theft or fraudulent use of the card, the device and/or the system of electronic identification and signature to the police authorities in the place where the loss or theft occurred within 24 hours of becoming aware of events.

VI.4.3.2 **Fraudulent use of the password, PIN number, including the itsme code and identification measures and signature**

Within the scope of the above restrictions, the following is considered to be gross negligence on the part of the subscriber:

- recording the password and/or PIN/itsme Code in a readable form on the device, on the card or on an object or document that the account holder keeps or carries together with the device and/or the card;
- disclosing the password and/or PIN/itsme Code to a third party;
- keeping the personal security features together with the card reader, giving or disclosing them to a third party.

The subscriber is not liable for gross negligence if violence is used against their person, property or family to obtain the password and/or PIN or any other identification means, or if there is a threat of immediate violence to their person, property or family.

VI.4.3.3. **Other instances of gross negligence**

Within the scope of the above restrictions, it may be considered gross negligence on the part of the subscriber if they enable the people listed below to use Easy Banking App, the signature and identification procedures or the personal security features as a result of failure to take adequate precautions or exercise due attention with regard to the device, password, PIN/itsme Code, card or signature and identification procedures (including recognition of their fingerprints / facial recognition):

- the account holder, co-holder or authorised user of an account which is linked to the transactions carried out using Easy Banking App;
- the spouse, cohabiting partner, guests or visitors (for either private or professional reasons) of the subscriber or account holder

- persons who work for or with the subscriber or account holder, whether or not as employees and irrespective of their status;
- the parents and relatives of the subscriber or account holder.

VI.4.4 **Responsibility for access to and use of the device**

Subscribers are responsible for access to the device which they use to access and make use of the Easy Banking App service.

In particular, they are responsible for having exclusive use of the device, as defined in Article VI.1, when activating the fingerprint or facial recognition function to use as a means of identification.

They are therefore fully liable for access to their profile(s) and for any transactions carried out on the account(s) linked to them by any persons whose fingerprints or face chracteristics are or will be recorded on their device.

In this context, recording fingerprint(s) or face characteristics belonging to anyone other than the subscriber on the device may constitute proof of gross negligence on their part.

VI.5. **Execution and irrevocable nature of orders sent using Easy Banking App**

Subscribers may not revoke an instruction to transfer funds issued by means of Easy Banking App once it has been received by the Bank.

However, if the transfer of funds was due to occur on a date agreed with the Bank, it may be revoked at the latest the day prior to the scheduled execution of the payment order.

A transfer with memo date or execution date may be cancelled electronically using the "Delete" function in the mobile application or in Easy Banking Web. The cancellation is signed using the signature means made available by the Bank.

The account holder irrevocably authorises the Bank to debit their account with the amount of the transactions carried out using the Easy Banking App. Any unauthorised negative balances which an account may display following these debits do not in any way constitute the granting of an overdraft, and must be settled immediately by the account holder.

Transmission of payment orders made using the Easy Banking App service shall be carried out by the Bank on the accounts it holds, provided that the account status and the agreements that govern the account permit this.

The nature of such orders is not in any way affected by the fact that Easy Banking App is used to send the orders to the Bank.

The subscriber is obliged to take every precaution to prevent any unwarranted payments; the bank shall not intervene in disputes arising in this respect between the subscriber and the third parties that are beneficiaries of such payments.

VI.6 **Security Measures – Minimum requirements regarding the device – Updates for mobile applications**

The subscriber acknowledges and accepts that a permanently secure browser environment is a basic requirement to access and use the Easy Banking App service and that the Bank cannot be held liable for a security risk caused by the subscriber's device, browser, operating system, internet connection, firewall, network, etc.

The subscriber shall ensure that the service is used according to the security rules on correct internet conduct and device protection and, if applicable, secure networks. These essential rules are available online at www.bnpparibasfortis.be >Security and at the website www.hellobank.be > Security.

Subscribers are also required and agree to comply with the security measures laid down in Article VI.1 when they activate the fingerprint or facial recognition function as a means of identification.

The Bank will inform the subscriber of the technical characteristics and minimum configuration required for the device used, to enable the Easy Banking App service to function correctly and securely.

The subscriber must apply updates and use the new versions of the mobile applications which are provided periodically by the Bank. If the subscriber's device is incompatible with the update/new version of the mobile applications, the subscriber will not be able to access the service. The update or new version of the mobile applications making access to the service impossible does not under any circumstances constitute termination, deactivation or suspension of the service by the Bank.

VI.7. **Precautionary advice**

The Bank recommends that the subscriber takes the precautionary measures set out in this article in relation to the use of Easy Banking App.

VI.7.1 **Precautionary measures regarding the password and PIN, including the itsme code**

Your password and PIN/itsme code must remain secret: do not disclose them to anyone else, not even a family member, a friend nor anyone supposedly acting with the best of intentions.

No one – including your bank, police authorities or insurance companies – is entitled to ask you for your password and/or PIN/itsme Code.

Never write your password and/or PIN/itsme Code down, even in coded form (by disguising it as a telephone number, for instance).

When entering your password and/or PIN/itsme Code, do so away from prying eyes. Always make sure that nobody can see what you are doing, e.g., by shielding the keypad with your hand. Do not let anyone distract you. If you notice anything out of the ordinary, inform the Bank immediately.

When choosing a new password, avoid combinations which are too obvious (for instance part of your first or last name, your partner's or pet's name, a date of birth with your initials, etc.); the same applies to your PIN (e.g. part of your date of birth, your telephone number, your postcode, etc.). Choosing the same PIN for all your cards or access codes may seem like an easy option, but poses an obvious risk.

If you have reason to believe that someone else knows your Easy Banking App password, change it immediately in the mobile application. If you can no longer access the service using your Easy Banking App password, call the Easy Banking Centre or the Hello Team immediately (their contact details can be found at www.bnpparibasfortis.be or www.hellobank.be).

Equally, if the confidentiality of your itsme Code has been compromised, change it immediately or block your itsme Account through the available Belgian Mobile ID channels.

VI.7.2 **Precautionary measures for the Easy Banking App service**

Do not leave your device unsupervised, especially when it is logged in to the Bank's computer. Close the program using the "Logout" button as soon as you are no longer using the Easy Banking App service. Read our security advice at www.bnpparibasfortis.be and www.hellobank.be.

Make you sure you have and retain sole access and use of your device by recording only your fingerprints and/or your face characteristics when you activate the fingerprint / facial recognition function as a means of identification.

Ensure that you retain exclusive control of your device by registering only your own fingerprints when you activate the fingerprint recognition function as an identification procedure.

VI.8. **Easy Banking App service: right of use and intellectual property**

Subscribers have a strictly personal, non-exclusive right to use the software and mobile applications made available by the Bank as part of the Easy Banking App service for the purposes of normal use. The software and mobile applications are the property (including the intellectual property) of the Bank and/or persons that have assigned the usage rights to the Bank. However, subscribers have no property rights or other intellectual rights.

All parties are strictly prohibited from using the software and mobile applications, and from using them or sharing them with or from another web application or IT program, including a mobile application, for example to extract information via the mobile application or perform transactions.

The concepts of the Easy Banking App mobile applications, their texts, graphical presentation, illustrations, formatting and other integral elements are the property of the Bank and may not under any circumstances be modified, reproduced or distributed without the prior written consent of the Bank.

Subscribers may not make the software or mobile applications available to third parties, in full or in part, for free or in exchange for payment; nor may they copy, translate, adapt, compile or modify the mobile application or some of its content in any way, without the explicit authorisation of the Bank.

Nevertheless, subscribers have the right to perform the operations that are necessary to use the mobile application in a way consistent with its purpose, such as loading, displaying or storing the mobile application.

The brands, names and logos, whether registered trademarks or not, in the Easy Banking App application, are the sole property of BNP Paribas Fortis, other companies of the BNP group or even of other companies, and may not be reproduced. Users cannot use them as metatags on websites.

VI.9 **Use of Third Party Providers services**

VI.9.1. Notwithstanding anything else to the contrary in these Terms and Conditions, the subscriber may instruct a third party provider to access information on the subscriber's accounts held with the Bank and that are accessible online and/or give the Bank the subscriber's instructions to make payment transactions from the subscriber's accounts held with the Bank and accessible online and/or query the Bank as to availability of funds on the bank accounts held with the Bank, accessible online and linked to a card-based payment instrument issued by that third party provider.

The subscriber must check that the third party provider is duly authorised as a credit institution or payment institution to provide in Belgium payment initiation and/or account information services and/or to request the confirmation of the availability of funds before making use of its services. Where the subscriber gives access toan identification and/or signature procedure to a third party other than an authorised third party provider, the Bank will assume the subscriber is authorising the Bank to give access to information on, and/or to initiate payments from, and/or to confirm the availability of funds on his/heronline accounts held with the Bank, and the subscriber willbe responsible for all paymentsas well as for any disclosures of data madeas a result of the actions of said third party.

Where the subscriber used an authorised third party payment intiation services provider, the subscriber shall address themselves to the Bank for notifying and rectifying an unauthorised or incorrectly executed payment transaction.

VI.9.2. Any instructions as referred to in subparagraph VI.9.1 to initiate a payment transaction and/or to access account information and/or to confirm the availability of funds shall be deemed to be valid instructions from the subscriber to the Bank for the purposes of these Terms and Conditions and shall be treated in the same way under these Terms and Conditions as an instruction given by the subscriber.

VI.9.3. The Bank reserves the right to refuse an instruction as referred to in subparagraph VI.9.2. in the same cases where the Bank has the right to refuse an instruction directly given by the subscriber.

VI.9.4. The Bank may deny access to the subscriber's accounts held with the Bank and therefore refuse an instruction as refered to in subparagraph VI.9.2. where there are justified and evidenced reasons relating to unauthorised use or fraudulent activities by the third party provider referred to in subparagraph VI.9.1. Before doing so, the Bank will inform the subscriber that it intends to deny access and gives its reasons for doing so, unless it is not reasonably practicable to do so, in which case the Bank will inform the subscriber immediately afterwards. In either case, the Bank will inform the subscriber in the manner in which it considers most appropriate in the circumstances and will not be obliged to inform the subscriber, where doing so would compromise its reasonable security measures or otherwise be unlawful. If the event the Bank denies access to the subscriber's accounts held with the Bank, it is required to notify the relevant authority that it has done so.

VII. **BANK'S OBLIGATIONS AND LIABILITY**

VII.1. **Internal transaction log**

The Bank shall keep an internal log of transactions carried out using accounts held with the Bank through the Easy Banking App for a period of ten years from 1 January following the date on which the transactions are carried out.

VII.2. **Proof of transactions carried out using Easy Banking App**

The essential data for any payment transaction initiated or executed by the Bank through the Easy Banking App service is recorded and stored. by the Bank in such a way that they can be reproduced in legible form on various types of media.

In the event of any dispute with the subscriber regarding any of these transactions, and without prejudice to any evidence to the contrary produced by the subscriber, where this latter acts in his/her capacity as consumer, the Bank shall provide proof:

- for transactions initiated by the bank: that the payment transaction was correctly authenticated and duly recorded;
- for transactions executed by the Bank: that the payment transaction was correctly authenticated, duly recorded and entered into the accounts

and that this transaction was not impacted by any technical deficiency or other deficiency.

VII.3. **Continuity of the Easy Banking App service**

The Bank shall use its best endeavours in designing and developing programs and software for accessing the Easy Banking App service.

It shall do everything in its power to ensure the continuity of the services and maintain the security of its systems. However, the Bank may, without being liable for compensation, suspend services in order to maintain equipment or the existing software, or to install new versions of the software, provided that such suspension is limited to a reasonable period of time.

VII.4. **Failure to execute transactions - erroneous execution of transactions - and unauthorised transactions originating from accounts held with the Bank**

Without prejudice to the obligations and liability of the subscriber set forth in Article VI, the bank is liable for:

- the failure to perform, or the incorrect performance of, transactions using the Easy Banking App service, via devices or using hardware approved by the Bank, regardless of whether or not these are controlled by the Bank;
- transactions carried out without the holder's authorisation, and any omissions or irregularities relating to the management of the services that are attributable to the Bank.

In all cases where the Bank is liable, pursuant to the first paragraph of this Article, it shall refund subscribers as soon as possible, as follows:

when, as a result of failure to perform a transaction, or the incorrect performance of a transaction, there is a loss equal to all or part of the transaction value, the amount of such loss plus any interest;

the amount required to return the user's situation to what it was prior to the unauthorised transaction, plus any interest on this amount;

with the amount of any other financial loss or charges, including charges paid by the subscriber to determine the amount for which compensation is payable;

the financial loss resulting from the user carrying out transactions incorrectly, if this is due to malfunction of the Easy Banking App service or any other equipment approved by the Bank, provided that such malfunction is not caused by the user, either deliberately or in breach of Article VI.1.

The Bank accepts no liability for any loss whatsoever, whether direct or indirect, arising either as a result of defective functioning of the customer's equipment or of telecommunication services provided by a third party, or as a result of the service being suspended for reasons beyond the Bank's control.

VII.5. **Providing information**

As part of the services, the Bank provides general and personalised information relating to accounts. The bank shall make every effort to provide accurate information.

This general information is gathered from the best sources available. Other than in the event of gross negligence or deliberate transgression of duty, the Bank cannot be held liable either in the event of certain information proving

inaccurate, or for the way in which account subscribers might interpret or use the information provided.

VIII **Easy Banking App –Evidences**

VIII.1 **Identification and/or signature means**

In addition to the Standard Terms and Conditions, in particular Article 22 thereof, the subscriber expressly agrees that any use of one or more of the identification and/or signature procedures enabling the user to access and use one or more of the Easy Banking App services, has the status of an electronic signature within the meaning of Article XII.15 of the Code of economic law.

The subscriber therefore expressly agrees that the electronic signature created using one or more of the identification and/or signature means constitutes, for both the account holder and the Bank, proof of the his or her identity, his or her agreement as to the content of transactions, orders and actions confirmed and/or transmitted using this signature, and constitutes confirmation that the transactions, orders and actions confirmed and/or transmitted by the subscriber and those received by the Bank are identical.

The subscriber agrees that this electronic signature is binding and accepts responsibility for the transactions, orders and actions confirmed and/or transmitted using this signature, without prejudice to Article VI of these General Terms and Conditions, and without prejudice to the subscriber's right as a consumer to produce evidence to the contrary if she or he alleges any error or irregularity.

VIII.2 **Participation by the Bank in producing evidence**

The essential data from any payment transaction initiated or executed by the Bank through the Easy Banking App service are recorded and stored by the Bank in such a way that they can be reproduced in legible form on any type of media.

In the event of any dispute with the subscriber regarding any of these transactions, and without prejudice to any evidence to the contrary produced by the subscriber, where this latter acts in his/her capacity as consumer, the Bank shall provide proof:

- for transactions initiated by the bank: that the payment transaction was correctly authenticated and duly recorded;
- for transactions executed by the Bank: that the payment transaction was correctly authenticated, duly recorded and entered into the accounts

and that this transaction was not impacted as the result of a technicaldeficiency or other deficiency.

VIII.3 **Recordings**

Recordings of phone communications defined in ArticleIV.1 shall be dealt with in accordance with the Bank's Privacy Notice.

The Bank keeps these recordings for 10 years, after which the records are destroyed, unless the Bank is obliged to keep them for longer on essential legal grounds, pursuant to regulations or on grounds of legitimate interest.

These recordings shall constitute complete evidence of the content of the call, including for orders and/or requests made by the subscriber. In the event of dispute, they may be produced as evidence before the body appointed to resolve the dispute.

When the phone communications relate to the services that the Bank markets for other entities, the Bank is authorised to send the recordings of these phone communications to the entity involved, for the purposes described above.

If the subscriber considers that there has been an error or irregularity in the recording system, they shall be required to prove this.

IX. **TERM OF THE AGREEMENT AND CANCELLATION OF THE EASY BANKING APP SERVICE**

This agreement is made for an indefinite period.

The subscriber, including the legal representative of subscribers under 18, may terminate the agreement at any time, without penalty, subject to one month's notice.

The Bank may terminate the agreement at any time by giving two months' notice. In the case of business use, the notice period is one month. However, the bank may terminate the service with immediate effect if the holder fails to honour one of their obligations towards the bank, or if the bank becomes aware of facts that jeopardise the relationship of trust and confidence between the holder and the bank.

Cancellation of the agreement relating to the Easy Banking Web service by the customer or the Bank, also leads ipso jure and under the same conditions, to the cancellation of the Easy Banking App agreement.

The subscriber, including the legal representative of subscribers under 18, may suspend access to the Easy Banking App service at any time and free of charge, by contacting the Easy Banking Centre Helpdesk (+32 2 433 41 90) for Easy Banking App mobile applications or the Hello Team (+32 2 433 41 45) for Hello bank! mobile applications.

The Bank reserves the right to suspend the holder's access to the Easy Banking App service or to any of its functionalities if:

- the service has been used for illicit or immoral purposes;
- the integrity, security (including by use of a device that has been jailbroken) or the reputation of the Bank and the Easy Banking App service have been compromised or are at risk of being compromised
- several incorrect passwords and/or PINs have been entered in succession;

- consecutive failure to recognise the digital fingerprints or facial recognition recorded on the subscriber's device;
- the subscriber has used the service in a way that is contrary to these General Terms and Conditions;
- the subscriber fails to honour one of their obligations towards the Bank, or the Bank becomes aware of facts that jeopardise the relationship of trust between the holder and the Bank;
- there is a risk of improper or fraudulent use.

If the subscriber's access to the Easy Banking Web service is suspended, the Bank reserves the right to also suspend the user's access to the Easy Banking App service.

Costs which are periodically levied in connection with this agreement are only due proportionally by holders until termination of the agreement.

X. **RATES FOR THE EASY BANKING APP SERVICE**

X.1 **Fee payable for the service**

Subscription is free.

X.2 **Other charges**

The following are or may be subject to charges:

- replacement card readers.
- the mobile payment referred to in Article IV4.

The subscriber to the Easy Banking App service will:

- pay the costs of purchasing, installing and running the mobile application, hardware or other equipment and the electronic identification and signature device enabling them to access the services
- pay the costs for connection to the Internet or other networks in Belgium and abroad according to the rates in force.

X.3 **Information about charges, credit or debit date and value dates**

Please refer to Chapter 3, "Payment Services" in the BNP Paribas Fortis General Terms and Conditions and the list of charges which is available to account holders in all the Bank's branches and on the Bank's websites www.bnpparibasfortis.be and www.hellobank.be.

XI. **COMPLAINTS AND APPEALS**

Complaints can be submitted to the Bank via the customer's branch or the Customer Services department, or by using the complaint form available in Easy Banking Web and at www.bnpparibasfortis.be and www.hellobank.be.

In the case of a disagreement over the Bank's proposed solution, the customer may refer to the Bank's Complaints Management Service by writing to:

BNP Paribas Fortis SA/NV

Complaints Management Service

Montagne du Parc 3

B -1000 Brussels

Should the customer be dissatisfied with the Complaints Management Service's proposed solution, an out of court settlement procedure may be initiated by contacting the following qualified entity:

OMBUDSFIN – Ombudsman in Financial conflicts

by writing to:

North Gate II

Boulevard du Roi Albert II 8 box 2

1000 Brussels

Fax: +32 2 545 77 79

E-mail: ombudsman@ombudsfin.be

or using an online form available from www.ombudsfin.be > Make a complaint

This website details the characteristics and conditions for initiating this out of court dispute settlement procedure, which the Bank uses by virtue of its Febelfin membership.

The customer may, if required, also make a complaint about a payment service by writing to:

Federal public service for Economy, SMEs, Middle Classes and Energy

Direction générale de l'Inspection économique

Services centraux – Front Office

North Gate III, 3ème étage

16 boulevard Roi Albert II

B -1000 Brussels

or via the online form available at: http://economie.fgov.be/en/disputes/complaints

As a consumer, you can also lodge a complaint relating to an online sale or service via the form available on the European Union website http://ec.europa.eu/odr.

The customer's right to pursue other legal remedies is not affected by initiating an out of court dispute settlement procedure as referred to above.

XII. **CHANGES TO THESE GENERAL TERMS AND CONDITIONS**

Subscribers shall be informed of any amendment to these General Terms and Conditions by means of a notice included with an account statement, by standard mail or by means of another hardcopy medium to which holders have access. This information will be provided at least two months before the amendment concerned takes effect.

When sending the information mentioned in the first paragraph, the bank shall also advise subscribers that they have a period of at least two months in which to terminate the contract, free of charge; if holders do not confirm termination within this period, they shall be deemed to have accepted the amended Terms and Conditions.

XIII. **PRIVACY**

XIII.1 **General**

The Bank processes the personal data of the subscriber in accordance with the terms of the Privacy Notice of BNP Paribas Fortis SA/NV available on https://www.bnpparibasfortis.com/footer-pages/privacy-policy and also at your disposal in all branches.

XIII.2 **Additional stipulations concerning Zoomit**

Please refer to Article 9 of the Zoomit service Regulations in Appendix 1 to the General Terms and Conditions for debit cards and Easy Banking Phone and Easy Banking Web services.

XIII.3 **Subscriber’s fingerprints or face characteristics**

The subscriber’s fingerprint(s) or face characteristics stored on his/her device are never shared in any form whatsoever with the Bank when the subscriber activates them in his/her profile and uses the fingerprint or facial recognition function as a means of identification on a device which supports this and on which the mobile application is installed.

These data are never processed by the Bank.

The mobile application only queries the function on the subscriber’s device and only receives back as data a confirmation from this that the fingerprint being offered or the face shown is recorded on the subscriber’s device.

The processing of the holder's personal details in the context of the fingerprint / facial recognition function is subject to the terms and conditions of the manufacturer of the compatible device