



GENERAL TERMS AND CONDITIONS RELATING TO DEBIT CARDS

Valid as from 15/01/2020

ARTICLE 1. GENERAL

In addition to the Standard Terms and Conditions, the services linked to a debit card shall be governed by these general terms and conditions.

These general terms and conditions are supplemented, where relevant, by technical instructions available at www.hellobank.be

In the event of contradiction between the Standard Terms and Conditions and these general terms and conditions, the latter shall prevail.

ARTICLE 2. DEFINITIONS

For the purposes of these general terms and conditions, the following terms are to be construed as defined below.

- **Account:** the account related to the transactions carried out using the Card in the framework of one or more services offered under this/these account(s) and subject to the powers accorded to the User thereunder;
- **Activation Code:** unique code which the User receives when ordering a new Card in his/her name which provides access to the secure telephone line where s/he may choose a personalised PIN (should s/he so wish) and activate his/her Card upon receipt;
- **Authentication Code:** code generated through the Card and the card reader (or through another item of equipment or process) and supplied to the User, allowing the Bank to verify the User's identity or the validity of the use of the Card;
- **Bank:** BNP Paribas Fortis SA/NV;
- **Card:** debit card issued by BNP Paribas Fortis under the Hello bank! brand;
- **CARD STOP:** company appointed by the Bank to receive all notices related to the loss, theft or risk of fraudulent use of a Card, a PIN or an Authentication Code;
- **Cash Deposit:** the possibility for the User to deposit euro bank notes on an Account through an ATM available for that purpose in a BNP Paribas Fortis branch;
- **Easy Banking Services:** Easy Banking Web/Easy Banking App and Easy Banking Phone;
- **Holder:** the natural or legal person, holder of the Account to which the Card, depending on the service in question, provides access ;
- **PIN:** personal and confidential ID number linked to the Card which the User shall use to identify him/herself in order to access the services linked to the Card;
- **User:** the natural person to whom a Card per account has been issued by the Bank. The User shall be either the Holder or an attorney-in-fact of the Holder. In the case of the latter, this power of attorney may be restricted by the User to use of the Card.

ARTICLE 3. DELIVERY AND ACTIVATION OF THE CARD – TERMS AND CONDITIONS OF USE

3.1. Delivery of the Card

Unless otherwise expressly requested by the User (or by the Holder, as a legal person), and subject to the following stipulations, the Card shall be sent to the most recent correspondence address provided by the User. It shall be blocked during despatch and may not be used until activated by the User.

Notwithstanding the above, the Card will be sent to the User's legal resident address if the User was identified remotely when entering into

relations with the Bank, until such time as his/her identity has been confirmed in person by a representative of the Bank.

Upon receipt, the User must immediately sign the strip on the back of the Card with indelible ink.

3.2. PIN and activation of the Card

When ordering a Card, the User shall receive an Activation Code which allows the User via a secure telephone line to:

- choose his/her PIN before delivery of the Card;
- activate the Card upon receipt, when the PIN is sent by the Bank.

The Card shall be disabled if three successive incorrect PINs are entered.

Where the Card is replaced at the User's request or renewed upon expiry, the new Card will be automatically activated the first time it is used with the existing PIN of the replaced or renewed Card. If a temporary card has been provided, pending a new Card, a PIN specific to this Card will be issued by the Bank.

3.3. First use of the Card

The first use of the Card:

- must consist of either a transaction requiring use of the PIN with a merchant or an ATM (a balance request on an Account suffices) or access to the Easy Banking Service;
- may not be for a payment on the Internet.

3.4. Subsequent uses of the Card

Any use of the Card requires, as a general rule, use of the PIN and where applicable, Authentication Codes.

In the event of business use of the Card, there is exemption from Article VII.44, §2 of the Code on Economic Law when the User has not been asked for a PIN or an Authentication Code.

ARTICLE 4. AVAILABLE SERVICES

The services described below may be activated on the Card, as the User chooses.

Activation shall constitute express confirmation by the User that s/he has read and accepted the rules, terms and conditions and charges applicable to such services, as amended from time to time. The User may request a copy on a durable medium at any time.

The Bank reserves the right to impose restrictions on access to the services, their functionality and any transactions thereunder with respect to Users who are identified remotely when entering into relations with the Bank, until such time as their identity has been confirmed in person by a representative of the Bank.

The terms and conditions of access to the various services are available at www.hellobank.be.

4.1. Cash withdrawals at ATMs and payments to merchants in Belgium and abroad

4.1.1. Principles

These services are automatically linked to each Card. They offer the User the option of withdrawing cash from the Bank's ATMs and from ATMs of other banks in Belgium and abroad, featuring the Bancontact, Maestro or Cirrus logos.

With his/her Card, the User may also pay for his/her purchases of goods or services from third parties who have terminals accepting payments in Belgium and abroad and featuring the Bancontact or Maestro logos.

Due to security considerations, the Bank may however impose restrictions on the terms of use of the Card in certain non-European countries. Further information about these restrictions can be obtained from customer services (Easy Banking Centre/Hello Team) or at www.hellobank.be.

When paying by Card at the outside payment terminal of a petrol station which only accepts payments for fuel, a fixed amount is reserved on the Card at the initiative of the petrol company for the strict time it takes to fill the vehicle with the fuel.

The exact amount due corresponding to the fuel consumed will be deducted from this reserved amount upon completion and the balance of the reserved amount will be simultaneously released.

4.1.2. Limits

Cash withdrawals from ATMs are limited as follows:

- Maximum amount per card and per day: (midnight to midnight):
EUR 625;
- maximum amount per card, per 7-day period:
EUR 1,250.

Payments in shops in Belgium and abroad (taken globally with the online payments referred to in Article 4.2) are limited to a maximum of EUR 2,500 per card per seven-day period. More details concerning these limits are available at www.hellobank.be.

Subject to the Bank's consent, the User (or the Holder) may increase or reduce the limits on cash withdrawals and/or payments for an unspecified period or for a specified period not exceeding 7 days.

This option shall not however be available for Users who were identified remotely when entering into relations with the Bank, until such time as his/her identity has been confirmed in person by a representative of the Bank.

In its battle against fraud, the Bank reserves the right to automatically and with immediate effect reduce a Card's limits, if necessary for certain merchants or specific sectors of activity should:

- the User fails to comply with the obligations arising from these general terms and conditions;
- the Bank's fraud detection systems indicate possible fraud on the Account(s);
- the conditions applied by the Bank in order to benefit from a certain limit no longer appear to be fulfilled upon an ulterior inspection.

Besides the limits described above, when payment transactions may be carried out using terminals not requiring a PIN (for example, by simple confirmation using an "OK" button or by contactless payment), such payments will be limited to an amount of EUR 25 per transaction and to an accumulated amount of EUR 50.

Without prejudice to the above, a limit of:

- EUR 50 shall apply at car park payment terminals (Maestro payment)
- EUR 100 shall apply at tolls (Maestro payment).

4.2. Online payments

The User may transmit a payment instruction to a merchant using the Card as part of an online transaction.

The applicable limits to the amounts of these transactions are set out in Article 4.1.2.

4.3. Cash Deposit

The User may use his/her Card to deposit euro bank notes, via automatic machines (Self Cash Deposit machines) specially designed for this

purpose and available in certain branches of the Bank, on an account held with the Bank:

- of which s/he is Holder, joint-holder or attorney-in-fact;
- of which s/he is the Holder's legal representative;
- which is linked to such Card.

To this end, s/he shall follow the instructions featuring on the machine's screens.

This option shall not however be available for Users who were identified remotely when entering into relations with the Bank, until such time as his/her identity has been confirmed in person by a representative of the Bank.

The Bank may establish limits on these deposits per transaction, per Card and per Account.

A specific and unique electronic verification is carried out on every bank note deposited in the Self Cash Deposit machines. Unless proved otherwise by the User or the Holder, this verification by the Bank shall constitute evidence of the recorded transaction.

False bank notes shall be withheld by the machine and shall not be credited to an Account.

4.4. Credit transfers

By identifying him/herself using his/her Card and associated PIN, the User may carry out credit transfers using certain terminals of the Bank.

Credit transfers to current accounts where the User is the (joint-)holder, attorney-in-fact, usufructuary or the legal representative of the account holder shall be limited to the available balance of the account to be debited.

In all other cases, they shall be limited to this balance, subject to a maximum amount of EUR 5,000 per day and EUR 10,000 per week. These limits shall also take into account credit transfers carried out using Easy Banking Phone.

4.5. Other specific services available via Bank terminals

By identifying him/herself using his/her Card and associated PIN, the User shall have access to various services, described at www.hellobank.be and/or on the screens of the terminals themselves (view balance, account history, change PIN, etc.).

The list of available services may evolve and any change will be communicated by the same means.

4.6. Access to Easy Banking Services

Subject to the conditions set out in the Standard Terms and Conditions and more specifically Appendix 1, or in any specific agreements, the Card may be used in the context of Authentication and/or Signature Procedures used to access various remote channels of the Bank, as well as to execute mobile payment transactions (depending on the remote channel concerned).

4.7. Third-party payment applications

The Bank allows the User to link his/her card to certain third-party payment applications through which s/he may initiate payment transactions linked to that Card (initiating these payments using Bancontact and/or Maestro shall be subject to the options selected in the relevant application allowing the use of Bancontact and/or Maestro). Specific transaction limits may apply. The User must accept the terms and conditions of use and the privacy policy provided by the editor of the relevant payment application, who provides such application to the User under its exclusive responsibility. The Bank is not a party to any agreement between the User and the editor of the relevant payment application.

The obligations and liabilities of the User and of the Holder, as set out in Article 5 of these general terms and conditions, notably in respect of security, confidentiality and notification of lost or stolen Cards or of any risk of unauthorised use of a Card or PIN, shall apply in their integrity to use of a third-party payment application. In this context, the term "Card"

used in these general terms and conditions shall also include the device on which the third-party payment application is installed, including, where applicable, the User's mobile device; the term "PIN" shall mean the security methods applied to the third-party payment application and/or the device on which the application is installed.

ARTICLE 5. OBLIGATIONS AND LIABILITY OF THE USER AND THE HOLDER

5.1. Control and security of the Card and PIN

The User is obliged to use the Card and the services to which it provides access in accordance with the terms and conditions governing the issue and use thereof.

The User is obliged to keep his/her PIN and Authentication Codes strictly confidential and to keep his/her Card, PIN and Authentication Codes under his/her exclusive control.

To this end, the User shall follow, amongst others, the below security advice:

- as soon as s/he receives his/her PIN, the User shall memorise it and, where applicable, destroy the document on which the PIN was sent;
- s/he shall not disclose his/her PIN or Authentication Codes to anyone, not even to a family member or to friends;
- s/he shall not write his/her PIN down, even in coded form, e.g. by hiding it in a false telephone number;
- s/he shall choose his/her PIN avoiding combinations that are too obvious (such as part of his/her date of birth, phone number, postcode, etc.) and refrain from using a code used for other services as his/her PIN;
- s/he shall enter his/her PIN away from prying eyes, making sure that s/he is never being observed and that s/he cannot be seen without his/her knowledge. If the User notices anything out of the ordinary, s/he must inform the Bank immediately;
- if the confidentiality of his/her PIN or Authentication Code is compromised, the User shall change it immediately.

No one – including the police authorities, insurance companies or the Bank – has the right to ask the User for his/her PIN or Authentication Codes, other than, with respect to the Bank, in accordance with the procedures described at www.hellobank.be and/or in the channels.

In any case, the User undertakes to follow the safety advice available at www.hellobank.be.

When the Card and the PIN or Authentication Codes are used as part of an authentication process in connection with an Easy Banking Service, the conditions of that Service shall also apply.

5.2. Notification in the event of loss or theft or risk of fraudulent use of the Card, PIN and/or Authentication Codes

The User or the Holder shall immediately notify CARD STOP (+32 70 334 344, 24/7) as soon as s/he becomes aware of the loss, theft or risk of fraudulent use of his/her Card, PIN or Authentication Codes.

Any events notified in accordance with this Article must be reported within twenty-four hours to the police authorities.

5.3. Liability in the case of fraudulent use of the Card, PIN or Authentication Codes

5.3.1. Until the time of notification

Until the time of notification as set out in Article 5.2, the Holder shall be liable for the consequences resulting from the loss, theft or fraudulent use of his/her Card, PIN or Authentication Codes, and of the User's Card, PIN or Authentication Codes, up to a maximum amount of EUR 50, except in the case of gross negligence or fraud, in which case this limit shall not apply.

By way of derogation the above paragraph, the Holder shall not bear any losses if:

1) the loss, theft or misappropriation of his/her Card, PIN or Authentication Codes or of the User's Card, PIN or Authentication Codes could not be detected by the Holder or the User before the payment made with the Card, unless one of them 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.

The limits on liability provided for in this article do not apply with regard to a Holder acting for professional purposes.

5.3.2. After notification

Once the notification as set out in Article 5.2 has been carried out, the Holder shall no longer be held liable for the consequences resulting from the loss or theft of his/her Card, PIN or Authentication Codes or of the User's Card, PIN or Authentication Codes, unless the Bank can prove that one of them has acted fraudulently.

5.3.3. Gross negligence

5.3.3.1. General

Depending on the factual circumstances and without prejudice to the discretion of the courts, the following shall be deemed to constitute gross negligence on the part of the User or Holder:

- failure to notify CARD STOP of the loss, theft or risk of fraudulent use of his/her Card, PIN or Authentication Codes;
- failure to familiarise him/herself regularly with the situation of his/her Accounts and the transactions recorded on them, if the consequence of this failure is to delay the detection and notification of fraudulent use of the Card, PIN or Authentication Codes;
- failure to follow the security advice set out in the Standard Terms and Conditions, these general terms and conditions or via the site www.hellobank.be, as well as communications issued by the Bank when sending out the Card;
- failure to report the loss or theft of his/her Card, PIN or Authentication Codes to the police authorities within 24 hours of becoming aware of events;.
- more generally, takes one of the actions set out in Articles 5.3.3.2 and 5.3.3.3.

5.3.3.2. Insufficient precautions in respect of the PIN and Authentication Codes

Within the limits set out above, the following may be deemed to constitute gross negligence on the part of the User:

- to write down the PIN in a readable form on the Card, on the device on which the Card is registered, or on an object or document that the User keeps or carries with the Card;
- to disclose the PIN or Authentication Code to a third party;
- due to lack of precautionary measures or vigilance concerning the Card, PIN or Authentication Codes, to allow the persons listed below to make use of them:
 - the Holder, joint-holder or attorney-in-fact of the Account to which pertains the transactions carried out with the Card;
 - the spouse, cohabiting partner, guests or visitors (for private or professional reasons) of the User or of the Holder;
 - people, whether employed or not and irrespective of their status, who work for, or are co-workers of, the User or of the Holder;
 - parents and relatives of the User or of the Holder

However, no gross negligence on the part of the User shall be deemed if the PIN or Authentication Codes are obtained by extortion, using violence against the User, his/her property or one of his/her immediate relatives or the threat of violence.

5.3.3.3. Insufficient precautions in respect of a Card

This clause applies in the event of fraudulent use of the Card without the PIN.

Within the limits set out above, leaving the Card unattended can be considered gross negligence, whether:

- at the work place, unless the Card is in a locked drawer or cabinet;
- in a vehicle, even parked in a private road, and irrespective of whether or not that vehicle is locked;
- in a public place or a place accessible to the public, unless the Card is in a locked drawer or cabinet;
- in a private place (including the place of residence) in the presence of several people besides the User, for example a reception, party (including family parties), conference, screening, exhibition, sports activity or competition, unless the Card is kept in a locked drawer or cabinet;
- in courtyards, entrances and gardens that are considered private property;
- in the common parts of a building covered by a co-ownership agreement;
- In any space, other than the place of residence, where the User lives on an occasional or temporary basis (hotel room, hospital or clinic, tent, camper van, caravan, mobile home, trailer, boat, for example), unless the Card has been placed in a safe which the owner or manager of the premises makes available to its customers, in a locked drawer or in a cabinet.

However, the User shall not be liable for gross negligence, if:

- the theft of the Card involves violence against the User's person or property or his/her relatives, or where there is an imminent threat of violence;
- when the theft of the Card is perpetrated at the place of residence of the User according to the conditions set out hereafter. Only the principal residence shall be deemed a residence for the purposes of this provision - excluding any second or holiday home owned by the User or the Holder and any student lodgings. The theft must involve breaking and entering, climbing, violence, threats or skeleton keys.

ARTICLE 6. THE BANK'S OBLIGATION AND LIABILITY

The Bank must comply with the following obligations:

- take suitable measures to guarantee the secrecy of the PIN;
- ensure the availability of the CARD STOP service referred to in Article 5.2;
- stop the Card from being used once a notification referred to in Article 5.2 has been issued.

The Bank bears the risks of delivery of the Card, the PIN or the Activation Code to the User.

ARTICLE 7. TERM OF THE AGREEMENT AND TERMINATION OF THE SERVICE

This agreement is made for an indefinite period.

However, the Card has a fixed period of validity, mentioned on the card itself. It shall automatically be renewed on expiry, unless the service has been terminated in accordance with this Article.

The User may terminate this agreement free of charge, at any time, subject to one month's prior notice.

The Bank may terminate the agreement at any time by giving two months' prior notice. In the case of business use, the notice period is one month.

When the User is not the Holder of the Account to which the Card is linked, this agreement shall automatically terminate when the Holder brings an end to the User's power of attorney which allowed the User to use the Card.

The Bank reserves the right to seize or refuse a Card and to also instruct the network of cash dispensers and payment terminals in Belgium or abroad and merchants to seize or refuse a Card, in the following circumstances:

- three incorrect PINs have been entered in succession;
- the Card is defective or damaged;

- the Card has been forgotten in the terminal;
- the User uses the Card or a service to which it provides access in a way that is contrary to these general terms and conditions;
- the User or the Holder fails to honour one of his/her obligations towards the Bank, or the Bank becomes aware of facts that jeopardise the relationship of trust and confidence between the User or Holder and the Bank;
- there is a risk of improper or fraudulent use.

The fees charged periodically pursuant to this agreement are only payable by the Holder on a pro rata temporis basis until termination of the agreement.

ARTICLE 8. CHARGES FOR THE SERVICES

The following are or may be subject to charges:

- management costs of the Card;
- all transactions carried out using the Card;
- delivery of a new Card;
- delivery of a new PIN;
- modification to the user limits of the Card;
- replacement of a lost or stolen Card;
- provision of a temporary card.

These charges are included in the list of charges available at www.hellobank.be.

These charges are irrespective of any additional charges which certain merchants or ATM operators may impose.

ARTICLE 9. CHANGES TO THESE GENERAL TERMS AND CONDITIONS

The User shall be informed of any amendment to these general terms and conditions by a notice attached to an account statement, by simple letter or other durable medium. This information shall be provided at least two months before the amendments concerned take effect.

When sending the information mentioned in the above paragraph, the Bank shall also advise the User that s/he has a period of at least two months in which to terminate the agreement, free of charge. If termination is not confirmed within this period, s/he shall be deemed to have accepted the amendments made to these general terms and conditions.