Belfius Bank SA/NV
Boulevard Pachéco 44 - 1000 Brussels
Tel. + 32 2 222 11 11 - www.belfius.be
RPM Brussels VAT BE 0403.201.185

General terms and conditions of use

(Unofficial translation)

Introduction

These general terms and conditions set out the respective rights, obligations and responsibilities of the Account Holder/Cardholder and of Belfius Bank SA/NV arising from the use of the Self-Service Banking, Bancontact / Mister Cash and Proton services and from the card scheme for which the logo is displayed on the front of the Card. They take precedence over the provisions of the Standard Terms of Business. These general terms and conditions are also sent out in hard-copy form to the Cardholder prior to the Cardholder signing the contract for the Card. All of the general terms and conditions and other regulations are also available, free of charge, from www.belfius.be or, upon request, from local branches.

Section I. General

Article 1 – Definitions

Account Holder: the natural person or legal entity who/which is the holder of the bank account on which the transactions carried out are entered and recorded.

Cardholder: the natural person to whom a Card has been issued.

The Bank: Belfius Bank SA/NV, whose registered office is situated at 44 Boulevard Pachéco, 1000 Brussels, RLE Brussels VAT BE 403.201.185

CBFA: the Banking, Finance and Insurance Commission, with which the Bank is registered under number 19649 A

The Card: the multifunction debit card that provides access to the automatic telling machines (ATMs) of Self-Service Banking, and/or the Bancontact / Mister Cash network, and/or the Proton system, and/or the Card scheme for which the logo is displayed on the front of the Card.

PIN Code: the secret code required for using the Card at the terminals provided for the purpose.

Self-Service Banking ATMs: the Bank's private network of ATMs, regardless of their name.

The Bancontact / Mister Cash Network: the network of Atos Worldline SA ATMs and payment terminals, as well as the other real and virtual systems accredited in Belgium.

The Network: the network of ATMs and payment terminals for the card scheme for which the logo is displayed on the front of the Card, as well as the other real and virtual systems accredited in Belgium and abroad.

The Proton System: the network of payment terminals and devices accredited in Belgium.

The Chip: the electronic circuit incorporated into a Card that records the available balance and the five most recent credit and debit transactions on the Proton system.

Mobile Banxafe: A service provided by the Bank in collaboration with the mobile phone carriers, enabling the holder of a Card to purchase call units or make secure payments using a mobile phone fitted with a Mobile Banxafe SIM Card.

Reference Exchange Rate: the exchange rate used to calculate exchange transactions and which is made available by the Bank at www.belfius.be.

Authorised Transaction: transaction consented to by the Cardholder/Account Holder in the manner set out in article 5 of these general terms and conditions.

Unauthorised Transaction: transaction not consented to by the Cardholder/Account Holder.

Article 2 – Issue of the Card and services relating to the Card

The Bank decides at its own discretion whether or not to issue a Card or to provide all or part of the services to which the Card provides access at the request of the Account Holder or representative. The Bank will refrain from sending out a Card automatically except where it is a renewed or replacement Card. The expiry date is shown on the Card. The Card expires on the final day of the month and year shown. Once the Holder receives/comes to collect his/her new Card, he/she is required to sign it in indelible ink and to render the old card unusable.

Article 3 – Secret code (PIN)

The Bank guarantees the secrecy of the PIN code linked to the Card. However, the Account Holder/Cardholder may not blame the Bank for not ensuring the confidentiality of his/her code/PIN if its disclosure is due to the fact that he/she has not complied with the Bank's recommendations regarding care and prudence. The PIN code is issued in line with the terms set out when the Card is issued. In principle, this PIN code will be selected and entered by the Cardholder at the terminals provided for this purpose when he/she comes to collect the Card from the branch. At the express request of the Holder, the PIN code may be sent out in a sealed and confidential envelope to the Cardholder's address. This PIN code is personal to the Cardholder.
The Cardholder may modify his/her secret code (PIN) using the terminals that the Bank makes available for this purpose. Should the Cardholder forget the code, he/she must ask the Bank for a new PIN. For the Mobile Banxafe service, the Customer will have an additional secret code for confirming transactions by mobile phone.

Article 4 – Terms for using the Card and consent

In order to carry out banking operations – view account balances, transfers, withdrawals and identifying himself/herself on the devices provided for this purpose, the Cardholder must insert the Card and enter his/her secret code (PIN Code) or, in some cases, sign a payment slip. Use of the Card may be restricted and/or be subject to additional conditions, for example for security reasons. The Cardholder should obtain any relevant information in this regard at his/her branch or by visiting the Bank's website at *www.belfius.be*.
The card and PIN Code will enable the Cardholder, where appropriate, to subscribe to the services provided electronically by the Bank to its Customers. The PIN Code replaces the Cardholder's handwritten signature. It also has the same probative value as a handwritten signature and provides proof that the Cardholder has given his/her consent to the operation, except where there is express authorisation stated otherwise in these Regulations.
When paying by Card at a petrol station, given that the exact amount of the payment is not known in advance, a certain fixed amount is reserved during the period strictly necessary for taking the fuel. Once the fuel has been taken, unless there is a technical error, the exact amount of the fuel taken will be deducted from the amount available for payments on the Card, while the amount reserved will be released immediately.

Transactions not requiring the entry of a PIN Code
Some terminals/devices (e.g. parking ticket machines) allow the Bancontact/Mister Cash network to be used for transactions with the Card that do not require the PIN Code to be entered. This means that some operations can be transacted simply by inserting the Card into the terminal, followed by confirmation given by pressing the OK button, or not. By carrying out this action, the Customer is deemed to have given consent for the transaction to take place.

FBPU 1527-5 1410

The amount per transaction may not be greater than 25 EUR and these operations can be combined up a maximum total of 50 EUR. After using his/her PIN Code, the Cardholder can then carry out transactions again not requiring a PIN Code to be entered on terminals/devices designed for this purpose and within the relevant limits.
The Cardholder can deactivate the Card's ability to conduct transactions without a PIN Code.

Article 5 – Description of possible uses

Card functionalities vary according to the system used and the type of device operating with the same system.

"Self-Service Banking" devices provide one or more of the following functions:

- viewing balances, printing account statements, deposits, cash withdrawals, transfers, ordering documents, changing the secret code, managing standing orders or direct debits,
- subject to special ad hoc authorisation from the Bank: withdrawals of amounts higher than the usual maximums, cash withdrawals from an account not linked to the Card (on condition that the Cardholder is authorised to make withdrawals from that account), cash deposits, cash withdrawals resulting from the closure of an account, cashing a cashier's cheque or any other transaction involving the handing over of cash. If the Cardholder wishes to make a cash withdrawal of more than 2,500 EUR, he/she must obtain information in advance about the notice required for these funds to be made available. Special ad hoc authorisation given by the Bank to withdraw cash from an account is always given subject to there being sufficient balance of funds available at the time the money is withdrawn using "Self-Service Banking" and subject to the occurrence of circumstances beyond the Bank's control or in the event of force majeure.
- access to Proton services: transferring money into (recharging) and emptying (discharging) the card, viewing "Proton" balances and mini-statement of the 5 most recent "Proton" transactions.
- depositing valuables into a night-safe. This function requires the Cardholder to make a specific request and is subject to special conditions. Only deposits in cash using banknotes of legal tender are accepted, whether they are deposited in a night-safe or via a "Self-Service Banking" terminal. Unless provision is made to the contrary, the deposit will be made into the account with which the Card is linked. In making use of the money-deposit system, the Customer agrees that the Bank's counting systems apply to him/her and that, as a result, the amount indicated on the bank statement takes precedence over the amount indicated by the Customer until such time as it is proved to the contrary.

The **Bancontact / Mister Cash system** allows for the following transactions: payments, cash withdrawals, viewing balances, changing the secret code, transferring funds to a Proton card, activation of the Mobile Banxafe service.
Transactions via the Network: payments and withdrawals of cash in Belgium, Europe and possibly outside Europe (see above).
The **Proton system**: payments and viewing account balances (see above).

Article 6 – Limits

The Cardholder or Account Holder may twice a year adjust the various upper limits, within the limits set by the Bank (annexe to the card application). The standard limits apply, except where the Bank or the Cardholder has indicated other limits. Subject to special authorisation from the Bank, the Cardholder may make withdrawals that fall outside the calculation of upper limits.

Article 7 – Transaction statements

At least once a month the Bank will make the following information available to the Account Holder for the transactions conducted using the Card: the transaction date, value date, identification of the transaction and, where applicable, information relating to the beneficiary; the amount debited, in euros and, where applicable, in foreign currency; commissions and charges relative to the transaction and recorded, as well as where applicable, the (reference) exchange rate used. If transactions are in foreign currency, the amount of the transaction is also stated by way of indication in euros. The conversion into EUR is made at the exchange rate used by the European Central Bank on the day the transaction was processed by the company/ merchant.

Article 8 – Transaction time

For transactions conducted on terminals placed under the Bank's control, the transaction is usually debited within a period of 5 days. For transactions conducted on other terminals, whether in Belgium or abroad, the Bank is reliant on the details being passed on by the organisations under whose control the terminals are placed. In exceptional circumstances, payment may be requested within the next year.

Article 9 – Charges

All charges linked to the Card and the services to which it provides access are stated in the document entitled Charges and Interest Rates for main financial services. This document is available in branches or from www.belfius.be. The Account Holder authorises the Bank to debit from the account any charges contractually due. Where applicable, some charges may be debited when the service is used for the first time. If the Customer wishes to avoid these charges being debited annually/quarterly/monthly, he/she must notify the Bank, giving one month's notice, that he/she wishes to cancel the Card or all or part of the services. Charges incurred regularly for the Card are only owed by the Account Holder/Cardholder pro rata for the period elapsed at the end of the contract. If these charges have been paid in advance, they will be reimbursed without delay pro rata from the month following the date of cancellation.

Article 10 – Cancellation of instructions

The PIN code replaces the handwritten signature. It also has the same probative value as a signature and serves as proof that the Cardholder has given his/her consent to the transaction.
The Cardholder may not revoke or cancel the instructions given using the Card when he/she has consented to the transaction by inserting his/her Card into the device provided for that purpose and entered his/her PIN code or else has carried out the authentication procedures required by the Bank to confirm the transaction initiated electronically.

Article 11 – Reimbursement of unauthorised or incorrectly executed transactions

Any Cardholder and/or Account Holder who notices a payment transaction that is either unauthorised or has been incorrectly executed is required to notify the Bank without delay and at the latest within thirteen months following the value date of the debit or credit. In the event of an unauthorised transaction, the Bank or Company will immediately reimburse the Account Holder/Cardholder for the amount of the unauthorised transaction, except where there is a clear presumption of fraud on the part of the Account Holder/Cardholder, or if the Account Holder/Cardholder has not complied with his/her obligations. Where applicable, the payment account that has been debited will be restored to the situation it would have been in had the unauthorised payment transaction not taken place, plus interest on this amount where appropriate. Any other charges will also be refunded. It is the responsibility of the Bank to prove that the payment transaction was authenticated, duly recorded and accounted for and that it was not carried out as the result of a technical defect or other problem.

Article 12 – Reimbursement of authorised transactions

The Cardholder/Account Holder is entitled to the reimbursement of an authorised transaction subject to the following conditions being met:

- the authorisation did not indicate the exact amount of the transaction when it was given; and
- the amount of the transaction exceeds the amount that the Account Holder/Cardholder might reasonably have expected, in view of his/her profile of past spending, from the conditions set under his/her contract and from the circumstances relating to the matter. However, for this second condition to apply, the Account Holder/Cardholder may not invoke reasons associated with a foreign exchange transaction if the reference exchange rate was

FBPU 1527-5 1410

applied. At the Bank's request, the Account Holder/Cardholder will provide the Bank with the factual elements relating to these conditions. The reimbursement will correspond to the total amount of the transaction carried out. The Cardholder/Account Holder may request reimbursement for an authorised transaction for a period of eight weeks from the date on which the amount was debited. Within a period of ten working days following receipt of a request for reimbursement the Bank will either reimburse the total amount of the transaction, or justify its refusal to reimburse. If the Customer, acting as a natural person for private purposes, is not satisfied with the response from the Bank, he/she should contact the Banks-Loans-Investments Mediation Service, 15-17 rue Belliard, box 8, 1040 Brussels.

Article 13 – Obligations of the Account Holder/ Cardholder

The Cardholder and/or Account Holder is required to comply with the following obligations:

- the Card has to be used in accordance with these terms and conditions and the terms of use have to be discovered either from the branch or from www.belfius.be;
- the Bank or Card Stop has to be notified immediately as soon as he/she becomes aware of the loss, theft or misuse of his/her Card, or any unauthorised use of his/her Card (Card Stop – telephone +32 70 344 344 – accessible 24 hours a day – address: Atos Worldline SA –1442 Chaussée de Haecht – 1130 Brussels);
- all reasonable measures have to be taken to keep the Card and personal security details safe, by for example, not allowing any third party (including his/her spouse, family member or friends) access to the secret code and/or to use the Card; to refrain from writing down his/her secret code in any form whatsoever;
- the Bank has to be notified immediately in writing of any change of address;
- the Bank has to be notified as soon as he/she becomes aware of any error or irregularity noted on his/her statement of expenditure, including the charging of transactions made without his/her consent.

Article 14 – Loss or theft

In the event of the loss, theft or misuse of the Card, the Cardholder will transmit to the Bank the reference number he/she was given when reporting the incident to Card Stop (see above), as well as a copy of his/her complaint to the relevant police services. If he/she has the Mobile Banxafe service, he/she will also be required to take these measures in the event of the loss or theft of his/her SIM card.
He/she agrees that the Bank or Atos will record his/her telephone statements and will use these recordings in the context of administering the proof.

Article 15 – Responsibility in the event of loss or theft

Provided the Cardholder has complied with the statutory provisions in the matter, as well as the conditions for issue and use, he/she will be responsible, before the loss or theft is reported, for the consequences associated with the loss or theft of the Card, up to an amount of 150 EUR. The Cardholder/Account Holder will benefit from this limit until notification of the loss or theft, even if the Cardholder has not managed to keep his/her personal security details safe.
His/her liability is not invoked if the Card has been used without being physically presented or without electronic identification, or if the Card has been copied by a third party or is used unlawfully, on condition that at the time of the transaction being disputed, the Cardholder/Account Holder was in possession of the card. If the Cardholder has acted fraudulently or has not fulfilled one or more of the obligations incumbent upon him/her after an act of gross negligence, he/she will be required to bear the cost of all losses arising from unauthorised transactions.

In particular, gross negligence includes:

a) the Cardholder making a note of his/her personal security details (such as his/her personal identification number or any other code) in an easily recognisable form and particularly on the Card or on an object or document kept or carried by the Cardholder with his/her Card;
b) the Cardholder not notifying Card Stop of the loss or theft of the Card as soon as he/she became aware of it. Loss also includes the Card being 'swallowed' by a terminal.

Depending on the circumstances and subject to the powers of discretion allocated to the person ruling on the matter, other incidents may also be deemed to constitute gross negligence irrespective of whether or not they result from the Cardholder not complying with his/her obligations under the General Terms and Conditions. In the event of the loss or theft of the Card, the holder of the rechargeable Proton instrument will himself/herself bear the consequences associated with the loss or theft of the Card, even after the Bank has been notified thereof. Notifying the loss or theft does not prevent the available balance being used. In the event of the Card being defective or if the Proton balance is not used up within a period of 6 months from the Card's expiration date, the Cardholder/Account Holder may return said Card to the Bank for the purpose of obtaining a refund of the balance. However, the Bank is not required to reimburse amounts lower than 10 EUR. The Customer may also discharge the Proton balance of his/her Card using Self-Service Banking ATMs.

Article 16 – Electronic journals

The Bank will keep an electronic journal or equivalent internal record of transactions carried out using the Card for 5 years from the time these transactions are carried out. For certain transactions, the ATM will issue a receipt stating the details entered by the Cardholder. This receipt records the transaction that the Cardholder entered at that particular ATM. It also provides information about the assumed balance of the account following that transaction, with the actual balance subject to any other transactions that may be pending.

Article 17 – Obligations of the Bank

The Bank is required to meet the following obligations:

- it must ensure that the personal security details of the Card do not become accessible to parties other than the Cardholder authorised to use the Card;
- it must refrain from sending out unsolicited Cards, except where a Card that has already been issued to the Cardholder/Account Holder needs to be replaced;
- it must make sure that the appropriate means are available at all times to enable the Cardholder/Account Holder to make the notification dealt with in Article 13 of these general terms and conditions, or to ask for the blocked Card to be released;
- it must be able to provide the Cardholder/Account Holder, when requested to do so and for 18 months from notification, the means of proving that he/she did in fact give that notification;
- it must prevent the Card from being used once notification has been given, in the sense of Article 13;
- it must bear the risk associated with sending a card to the Cardholder or any other means that enables him/her to use it and in particular any personalised security details;
- it must maintain an internal register of transactions for a period of at least five years from the time the transactions were carried out.

Article 18 – Responsibility of the Bank

The Bank will be responsible for the risk of sending out the Card or Code until such time as the cardholder receives it.
The Bank will be responsible for:

– failure to carry out, or failure to carry out properly, any transactions enacted using the Card from devices, terminals or equipment approved by the Bank, whether they are placed under the Bank's control or not;
– transactions enacted without the authorisation of the Cardholder;
– any error or irregularity made in the management of his/her account and for any counterfeiting of the Card, except where the irregularity, failure to carry out, or failure to carry out properly, is attributable to the Cardholder. As soon as the Bank is notified of the loss or theft of the Card, this will prevent any further use of the Card. In the event of a transaction carried out using the Card being disputed, the Bank will provide proof that the transaction was correctly recorded and accounted for and that it was not the result of a technical incident. If it is the responsibility of the Bank, the

FBPU 1527-5 1410

Bank will pay the Account Holder for the amount of the transaction not carried out or carried out incorrectly, or the amount required to restore the Account Holder's account to the situation it was in before the unauthorised transaction or counterfeiting of his/her Card, plus where appropriate any interest on these amounts, as well as other financial consequences such as assessment charges or the amount of the loss caused by the device, terminal or equipment approved by the Bank that malfunctioned.

Article 19 – Withdrawal or freezing of the Card and cancellation of the services associated with it

The Cardholder/Account Holder may, at any time and without charge, terminate the contract with immediate effect by giving notice of one month. In such cases, he/she is required to destroy the card and notify the Bank accordingly. In the same way, the Bank may at any time suspend or terminate use of the Card, or all or part of the services linked to it, by giving notice of two months. Charges regularly allocated to the Card are only owed by the Cardholder/Account Holder pro rata to the period elapsed at the end of the contract. If these charges have been paid in advance, they will be reimbursed without delay, pro rata, from the month following the date of cancellation. The Bank may block the Card for objectively justified reasons relating to the security of the Card (e.g. three successive incorrect attempts to enter a code number, report of the loss, theft or unlawful use of the Card, forgetting the Card at a service desk or in a terminal) or the presumption of unauthorised or fraudulent use of the Card (e.g. in the event of the Card being lost or stolen, or if the Card is used without complying with these Standard Terms & Conditions or the Bank's other requirements). The Bank will notify the Cardholder/Account Holder that the Card has been blocked, if possible before the Card is blocked and at the latest as soon as possible thereafter.
The Bank will not provide the information dealt with in the paragraph above if it is not possible, for objectively justified security reasons, to provide this information or if such information is not permitted under an applicable piece of legislation. The Bank will release the block on the Card or replace it as soon as the reasons for it being blocked in the first instance have ceased to exist. In the cases mentioned above, any transaction carried out using the Card may be declined and the Card may be 'swallowed' by the terminal.

Article 20 – Modification of the terms and conditions

In line with its General Terms and Conditions, the Bank may make changes to these general terms and conditions. These modifications will come into effect at the end of a period of 2 months from the date on which the changes were notified to the Cardholder, except where he/she has terminated his/her contract within the same period and destroyed his/her Card. Changes may also be made to the exchange rate with immediate effect, provided they are based on the reference exchange rate. Changes to interest or exchange rates that work in favour of the Customer may be applied without notification.

Article 21 – Protection of privacy

Belfius Bank and the entities of the Belfius Group, as well as the companies to which the Bank is linked by contract, use the Cardholder's/Account Holder's personal data, including information about payment transactions, the Customer's assets and personal details about his/her spouse and members of his/her family who live at the same address, for the purpose of managing their accounts, investments, insurance policies, loans or other products, as well as for offering the Customer financial, insurance or appropriate related products and services, and for assessing the relationship with the Customer and his/her spouse. This data may also be processed for the purposes of avoiding misuse, detecting fraud, managing disputes and verifying that the Bank's staff, delegated banking agents and persons employed by its delegated banking agents are complying with the obligations incumbent upon them under the law, their employment contract or their mandate as delegated banking agents, in particular in the area of donations, powers of attorney, etc. To guarantee the quality of this personal data, the Bank may call on third parties to supplement or amend this data.
Processing may include the transmission or exchange of data between certain entities in the Belfius Group. When the Bank works with third parties that process Customer data, these parties undertake to respect the confidentiality of the data. The Bank will take any measures required to ensure that these third parties respect the confidentiality of this data and guarantee its security, in particular when this collaboration involves the transfer of data of a personal nature to countries located outside the European Union where the legislation does not offer a level of protection for data that is equivalent to the level that applies in Belgium or within the European Union.
The Account Holder/Cardholder may at any time object to the use of his/her personal data for direct marketing purposes, either by writing to the Bank (Customer Management, 44 Boulevard Pachéco, 1000 Brussels) or by lodging a request at a branch using the "Identification Data of a Customer who is a Natural Person" document. He/she may exercise his/her right to access or amend his/her data by writing to the same address, attaching a copy of the front of his/her identity card to the letter. For security reasons, the Bank's premises and its Self-Service Banking and Bancontact / Mister Cash system ATMs may be placed under camera surveillance. The data from these cameras is processed in order to ensure the safety and security of persons and assets.

FBPU 1527-5 1410

Section II. Bancontact-Mister Cash App

A. Stand alone

Article 22 – General

These general terms and conditions govern the use of the Bancontact-Mister Cash App. The Bank acts as the distributor of the App. Section II of these general terms and conditions details the rights and obligations arising from the use of the App, both for the Customer and for the Bank. Insofar as no exemption is made in this section, section I of these general terms and conditions, as well as the General Terms of Business and the conditions accepted on downloading the App, continue to apply to transactions carried out using the App.
The definitions stated in section I continue to apply in section II and are supplemented by the definitions set out below.

Definitions:
- **"App"**: BC-MC mobile payment application;
- **"App User"**: any person who has installed the App on his/her mobile device and who holds a BC-MC card issued by the App Distributor;
- **"App PIN"**: the secret code consisting of four numbers that the App User may choose at will to identify himself/herself and to authorise Mobile Payment Transactions;
- **"App Distributor"**: refers to Belfius Bank SA, whose registered office is situated at 44 Boulevard Pachéco, 1000 Brussels, RLE Brussels VAT BE 403.201.185;
- **"BC-MC"**: refers to Bancontact-Mister Cash S.A., whose registered office is situated at 82 rue d'Arlon, 1040 Brussels, registered with the Crossroads Bank for Enterprises under number 0884.499.250 (RLE Brussels);
- **"Payee"**: an App User wishing to receive a payment by way of a Mobile Payment Transaction;
- **"Payer"**: an App User wishing to make a payment by way of a Mobile Payment Transaction;
- **"Services"**: the current and future services provided by the App Distributor to the App User enabling the App User to carry out Mobile Payment Transactions (make or receive payments, or both);
- **"Mobile Payment Transaction"**: action initiated by the Payee involving the transfer of funds (in EUR), regardless of whether there are underlying obligations between the Payer and Payee, or not.

Article 23 – Availability and operation of the App – Approval of transactions

23.1 Availability of the App
The App Distributor guarantees that it will act to the best effect in the context of making the App and Services available to the App User. However, the App Distributor is unable to guarantee that the App will function flawlessly and without interruption at all times. From time to time, the App may function slowly, be unavailable or not operate correctly as the result of various factors, including the location, speed of the Internet connection, technical reasons, maintenance or upgrades. The App is available through the App User's mobile device when that device is within range of a wireless network. The quality of the Services may vary, depending on the mobile device. The App Distributor and BC-MC reserve the right at any time and from time to time, to interrupt, limit, modify or stop the App (or any element thereof) temporarily for a limited period.

23.2. Operation of the App – Approval of transactions
Every Mobile Payment Transaction to be debited from the payment account linked to the Payer's Card must be authorised separately and transmitted to the App Distributor after the Payer has given his/her consent. Consent is only deemed to have been given for a Mobile Payment Transaction once the Payer has confirmed the transaction using his/her App PIN. The App User acknowledges the validity of the Mobile Payment Transactions made using the App and that he/she has authorised the payment with his/her App PIN. The App will be blocked if the App User enters an incorrect App PIN three consecutive times. To unblock the App, the App User will have to reactivate the App. If the Card is blocked, the App will also be blocked.
The Payer cannot cancel a Mobile Payment Transaction sent using the App if he/she has confirmed the transaction with his/her App PIN, in accordance with article 23.2. A Mobile Payment Transaction is deemed to have been received by the App Distributor when the App displays the amount of the Mobile Payment Transaction and the message "Thank you. Your payment has been made" on the Payer's mobile device.
All Mobile Payment Transactions initiated by the Payee using the App and authorised by the Payer with the App PIN will be carried out by the App Distributor at the end of the working day following the authorisation of the Mobile Payment Transaction by the Payer, on condition that the status of the Payer's account and the general terms and conditions that govern the payment account and the Payer's Card allow the transaction. Using the App to initiate Mobile Payment Transactions does not change the nature of such a payment transaction into a specific type of transaction by card. Mobile Payment Transactions can only be carried out using the App if both the Payer and the Payee are App Users.

Article 24 – Obligations of the App User

The App User is required to use the App and his/her App PIN in accordance with the provisions of these general terms and conditions. The App User must notify the App Distributor immediately of any unauthorised or incorrect transaction carried out using the App recorded in the App User's account statements. This means that the App User is required to view his/her account statements regularly in order to do so. The App User must notify CARD STOP immediately by calling 070/344 344 if there is a risk of the App PIN being misused and/or the theft or loss of his/her mobile device on which the App is installed. This notification must be made in accordance with these general terms and conditions.

Article 25 – Blocking the App

The App Distributor may block access to the App for objectively justified reasons associated with the security of the App if it suspects any unauthorised or fraudulent usage of the App or App PIN. If this should be the case and in accordance with the agreed methods, the App Distributor will notify the App User about the App being blocked and the reason why, if possible before the App is blocked or immediately afterwards. This notification is not required if not permitted under the law or if it is contrary to public security. The App Distributor will remove the block on the App once the reasons for it being blocked have passed and will notify the App User as soon as possible.
If and immediately after the App User has notified CARD STOP in accordance with these general terms and conditions, CARD STOP will block all use of the App.

Article 26 – Security measures

The App PIN is strictly personal and confidential and must be kept in a safe place by the App User. The App User must take all reasonable measures to keep his/her App PIN safe and, in this regard, he/she must respect the following security measures, including the security advice stated in the general terms and conditions:
- The App User may not leave his/her mobile device on which the App is installed or his/her App PIN unattended and he/she may not pass on details of his/her App PIN to other people or allow other people to use it;
- The App User must not make a physical note of his/her App PIN or keep it on any durable medium;
- The App PIN must be entered discreetly. To this end, the App User must ensure that no one else can see the App PIN when he/she enters it. He/she must also notify the App Distributor if he/she notes any unusual behaviour.

The conditions relative to (the use of) the payment instruments detailed in the general terms and conditions apply to the mobile device on which the App has been installed. The App User undertakes to ensure that his/her mobile device on which the App is installed meets the security standards stated at the App Distributor's website. To this end, the App User will comply with the protective systems built into his/her mobile device so that he/she can use the App in total security. If the App User deliberately disables these protective systems, the App Distributor cannot be held liable for any resulting damage.

Article 27 – Limitation of the App User's liability

In the event of the loss or theft of the mobile device on which the App is installed or if the App PIN is lost or misused, the App User will assume liability for any risk resulting from the unlawful use of the App

FBPU 1527-5 1410

PIN until such time as CARD STOP has been notified, in accordance with article 25.
However, the App User's liability is limited to 150 EUR per incident resulting from an unauthorised Mobile Payment Transaction. This limitation does not apply and the App User is liable for all damage or loss resulting from his/her own fraudulent or intentional act or gross negligence.
The courts will decide in the final instance whether the facts or actions of the App User, in the given circumstances, constitute an intentional act or gross negligence. The following circumstances may be considered as gross negligence, although the courts will not be bound by such qualifications:

- Passing on his/her App PIN to other people;
- Allowing other people to use the App on his/her mobile device;
- Leaving his/her mobile device on which the App is installed and/or his/her App PIN unattended in areas accessible to the public;
- Not immediately reporting the loss or theft of his/her mobile device on which the App is installed or his/her App PIN;
- If the App User fails to notify the App Distributor immediately of an entry in his/her account statements of any transaction for which no authorisation has been given or of any error or irregularity noted in the account statements.

The App User is not responsible for any damage or losses resulting from the loss or theft of his/her mobile device on which the App is installed or of any misuse of the App PIN that occurs after notification to CARD STOP, except where there is fraudulent use by the App User.

Article 28 – Responsibility of the App Distributor

The App Distributor is not responsible for:

(i) Any damage or modification to the App User's equipment by which (but not limited to) the portable device or mobile telephone, following the installation, upgrade, update or use of the App;
(ii) The temporary unavailability, suspension, interruption or delay in one or more Services following scheduled maintenance works, breakdowns or cases of force majeure, or for reasons beyond the reasonable control of the App Distributor;
(iii) Damage resulting from a difficulty or inability to load the App or access the contents of the App, or any other error in the telecommunication system that results in the App being unavailable;
(iv) Damage resulting from the unavailability of websites or information from third parties included as hyperlinks to the App, as stated in article 31, or resulting from the incorrect, incomplete or inaccurate nature of the information provided by third parties. Furthermore, nor may such external information give rise to any undertaking on the part of the App Distributor;
(v) Direct or indirect damage resulting from or related to the (poor) functioning of the App User's mobile device, or the telecommunication services or software or hardware of a third party.

Under no circumstances will the App Distributor be liable for any indirect damage suffered by the App User due to a breach of these general terms and conditions by the App Distributor, including loss of earnings, damage, loss of assets, customers, contracts, goodwill, data, actions by third parties, or any consequential or indirect loss or damage. Any such liability is excluded, whether contractual, non-contractual, foreseeable, known, scheduled or of any other nature.
The provisions of this article 28 do not limit the liability of the App Distributor in the event of misdemeanour or intentional fraud on its part.

Article 29 – Data protection

The App Distributor will gather all data of a personal nature (including the name of the App User, the activation code, Card number, expiry date and PIN Code, the data relative to the mobile device, including an impression of the mobile device and other technical information, in particular the technical information about the mobile device, telephone number, mobile applications on the device, name of the device, e-mail address installed on the telephone, identifier, OS version, name of the telecoms operator, telephone number, SIM card number, etc.), and process it in the context of or for the purpose of loading and installing the App, registering, using and accessing the App. All data of a personal nature will be gathered and processed by the App Distributor as the party responsible for its processing, in accordance with the Act of 8 December 1992 relative to the protection of privacy with regard to the processing of personal data (the "Privacy Act"). For the purposes set out above, the App Distributor may use the services provided by BC-MC, or by any other purveyor of external services which may act for and under the instructions of the App Distributor. The App Distributor will take appropriate technical and organisational measures and will ensure that BC-MC or any other purveyor of external services also takes appropriate technical and organisational measures to ensure that the App User's personal data is processed in total security and that it remains confidential. The App User has the right to access any personal data pertaining to him/her that may have been gathered and processed and also has the right to have any incorrect details amended. The App User may also object at any time, free of charge, to the processing of his/her personal data for promotional purposes. To exercise these rights, the App User should contact the App Distributor, as set out in article 21 of these general terms and conditions. The App User agrees only to submit accurate, current and complete details to the App Distributor, as required to register for the App. The App User also agrees to update his/her details so that they remain accurate, current and complete. The App Distributor reserves the right to terminate the App User's right of use if the information the App User has provided are incorrect, inaccurate or incomplete.

Article 30 – Intellectual property rights and licences

The App has been developed by and is the property of BC-MC, which has granted the App Distributor a licence to distribute the App to App Users. All trademarks, service marks, names, symbols and logos contain in or on the App are the property of BC-MC and its licensors.

Article 31 – External links

The App may include hyperlinks to third-party websites or information. The App Distributor has no control over third-party websites or information.

Article 32 – Cessation

The App Distributor may cancel use of the App at any time subject to notifying the App User of the cancellation two (2) months prior to the date of cessation by way of an account statement, letter or other durable medium. The App User may terminate use of the App free of charge at any time by uninstalling the App from his/her mobile device, without notification to this effect being required.
The App Distributor reserves the right to suspend the App User's access to the App if:

- The App User does not use the App in accordance with the general terms and conditions;
- The App Distributor becomes aware of facts that seriously harm the App Distributor's trust in the App User;
- There is a risk of misuse or fraud.

FBPU 1527-5 1410

B. Via Belfius Direct Mobile

Article 33 – General

These general terms and conditions govern the use of the Bancontact–MisterCash App that is part of Belfius Direct Mobile. Provided nothing to the contrary is stated in this Part B, Part A of Section II will continue to apply to transactions carried out using the Bancontact–MisterCash function in Belfius Direct Mobile.
The version of the Bancontact–MisterCash App that is part of Belfius Direct Mobile does not use an App PIN. However, Payers will approve their Mobile Payment Transactions by entering their individual security details for Belfius Direct Mobile.

Article 34 – Operating the App – Approving Mobile Payment Transactions

Any Mobile Payment Transaction to be debited from the payment account linked to the Payer's Card must be approved separately and transferred to the App Distributor after being approved by the Payer.
Approval of a Mobile Payment Transaction is only deemed to have been granted once the Payer has approved the Transaction by entering his or her individual security details for Belfius Direct Mobile.
The App User acknowledges the validity of the Mobile Payment Transactions carried out via the App and approved by him or her using his or her individual security details for Belfius Direct Mobile.
The App will be blocked if the App User enters incorrect individual security details for Belfius Direct Mobile on five consecutive occasions. In order to have the App unblocked again, the App User is required to reactivate Belfius Direct Mobile.
The Payer may not cancel a Mobile Payment Transaction sent via the App once he or she has confirmed the Transaction with his or her individual security details for Belfius Direct Mobile, in accordance with article 34. Mobile Payment Transactions will be executed by the App Distributor at the end of the working day following approval of the Mobile Payment Transaction by the Payer, on condition that the status of the Payer's payment account and the general terms and conditions governing this payment account and the Payer's Card allow it. Using the App to initiate Mobile Payment Transactions does not alter the nature of such a payment transaction as a specific card transaction. Mobile Payment Transactions may only be carried out via the App if both the Payer and the Payee are App Users.

Article 35 – Obligations of the App User – Blocking the App

The App User is required to use the App and his or her individual security details for Belfius Direct Mobile in accordance with the stipulations of these general terms and conditions, as well as in accordance with section 5, part II ("Belfius Direct Mobile application") of the Internet Banking Regulations.

FBPU 1527-5 1410

Belfius Bank SA/NV
Boulevard Pachéco 44 - 1000 Brussels
Tel. + 32 2 222 11 11 - www.belfius.be
RPM Brussels VAT BE 0403.201.185

+ Addenda when applying for a debit card

Services:

In principle, the following services are provided: Self-Service Banking, Bancontact/Mister Cash, Proton, withdrawals and payments via the card scheme whose logo is displayed on the front of the Card.
For savings accounts linked to debit cards, only transactions carried out via Self-Service Banking may be made with the Card. Both the Cardholder and the Bank may decline certain services.

Limits:

Standard limits:

Type of transaction	*up to age 16*	*from age 16*
Daily limit withdrawals	€ 100	€ 650(1)
Weekly limit withdrawals and payments	€ 100	€ 2.500(1)

The Holder or, where applicable, his/her legal representative(s) may modify these limits if they wish. If the Cardholder has signatory powers that are less than the limit for the Card, this limit will be the same as the amount for the signatory power. With certain ATMs, the limits shown above may be restricted.

Limits for underage users:

When the Cardholder reaches the age of 16, the Bank automatically applies the limits for that age. The Bank will notify the Cardholder of this by an attachment to the card statements.

(1) A maximum of 120 EUR may be withdrawn per month from a savings account opened by an underage Customer aged between 16 and 18. This is a statutory limit that it is not possible to modify.

Limits for transfers and standing orders:

Up to the age of 16

Limit category	*To other accounts*		*From a current account to accounts at Belfius Bank over which the Cardholder has a role as (co-)holder or proxy*		*From a savings account to accounts at Belfius Bank over which the Cardholder has a role as (co-)holder or proxy*	
	Per day	Per week	Per day	Per week	Per day	Per week
21	€ 0	€ 0	/	/	/	/
22	€ 20	€ 20	/	/	/	/
23	€ 50	€ 50	/	/	/	/
24	€ 100	€ 100	/	/	/	/
25	€ 200	€ 200	/	/	/	/

From age 16

Limit category	*To other accounts*		*From a current account to accounts at Belfius Bank over which the Cardholder has a role as (co-)holder or proxy*		*From a savings account to accounts at Belfius Bank over which the Cardholder has a role as (co-)holder or proxy*	
	Per day	Per week	Per day	Per week	Per day	Per week
1	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
2	€ 0	€ 0	€ 2,500	€ 7,500	€ 2,500	€ 7,500
3	€ 500	€ 1,500	€ 1,000	€ 3,000	€ 1,000	€ 3,000
4	€ 1,000	€ 3,000	€ 2,000	€ 6,000	€ 2,000	€ 6,000
5	€ 2,500	€ 7,500	€ 5,000	€ 15,000	€ 5,000	€ 15,000
6	€ 5,000	€ 15,000	€ 12,000	€ 36,000	€ 12,000	€ 36,000
7	€ 7,500	€ 22,500	€ 15,000	€ 45,000	€ 15,000	€ 45,000
8	€ 10,000	€ 30,000	€ 20,000	€ 60,000	€ 20,000	€ 60,000
9	€ 25,000	€ 75,000	€ 50,000	€ 150,000	€ 50,000	€ 150,000
10	€ 40,000	€ 120,000	€ 80,000	€ 240,000	€ 80,000	€ 240,000

FBPU 1527-5 1410