GENERAL TERMS AND CONDITIONS OF BANK CARD SERVICES, EASY BANKING PHONE AND EASY BANKING WEB valid from September 11th, 2017

I. GENERAL

The services Cash Withdrawal at our ATMs and paying in shops (POS) home and abroad, Cash Withdrawal at other ATMs, Self, statement printer, Cash deposit linked to a bank card, and the Easy Banking Phone and Easy Banking Web services are governed by the General Terms and Conditions of BNP Paribas Fortis SA/NV, with registered office at Montagne du Parc/ Warandeberg 3, B-1000 Brussels, Brussels RPM/RPR, VAT BE 0403.199.702, BFIC accreditation number 25879A.

In accordance with these General Terms and Conditions, the specific terms and conditions for the Cash Withdrawal at our ATMs and paying in shops (POS) home and abroad, Cash Withdrawal at other ATMs, Self, statement printer, Cash deposit linked to a bank card, and the Easy Banking Phone and Easy Banking Web services, are set out in these General Terms and Conditions, and also in the contract entered into by the holder, the technical manuals and appendices, and any notices of amendment sent to holders in accordance with the procedures stipulated in Article XII below.

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

These General Terms and Conditions do not apply to MasterCard, Visa or Access Cards issued by Fortis Bank SA/NV.

II. DEFINITIONS

In these General Terms and Conditions, the following terms are to be construed as defined below:

- Bank: BNP Paribas Fortis SA/NV, hereinafter referred to as "the Bank" or "BNP Paribas Fortis SA/NV", acting on its own behalf and, in this instance, acting for other entities that may or may not be part of the BNP Paribas Group, in which capacity the bank acts as an intermediary, subcontractor or partner;
- Bank card: bank card issued by BNP Paribas Fortis SA/NV, under the BNP Paribas Fortis brand or Hello bank!, and on which one or more of the following services have been activated: Cash Withdrawal at our ATMs and paying in shops (POS) home and abroad, Cash Withdrawal at other ATMs, Self, statement printer, cash deposit;
- our ATMs: ATMs made available by BNP Paribas Fortis in Belgium on behalf of its commercial entities, BNP Paribas Fortis and Fintro, bearing the logo of either of these entities;
- other ATMs: ATMs made available in Belgium by financial institutions other than BNP Paribas Fortis SA/NV and all ATMs abroad.
- POS: Point Of Sale/shop;
- online banking services: Easy Banking Phone and Easy Banking Web;
- holder: the natural or legal person to whom the Bank has issued the card; the natural person with access to an online banking service;
- account, current account, savings account: account, current account or savings account to which transactions carried out under one or more of the services are booked;
- account holder: holder – a natural or legal person – of the account, current account or savings account;
- authorised card user: person who is authorised to hold or use a card subject to certain limits;
- bank notes to his current or savings account through an ATM available to this end at a BNP Paribas Fortis branch;
- Photo card: bank card whereby the card holder has personalised the front of his card;
- Named card; bank card on which the personal details (account number, name) are stated.
- Temporary card: bank card without any personal details shown on the card itself, that the cardholder can obtain from the Bank's branches in the case of loss, theft or a technical fault with their own card, other than their Hello Bank card, and that, in expectation of receiving a new named card, may be used for a limited period. In order to use the temporary card the cardholder also receives a specific PIN code that may be changed by the cardholder at an ATM.
- available balance of the account: amount obtained by adding together the balance for the account and the amount of any credit or overdraft facilities granted by the Bank on the account concerned;
- Initial code: a unique code that the account holder receives when ordering their new card, giving them access to the secure telephone line in order to choose their own PIN (should they so wish) or to activate their card after receiving their card (having opted for the Bank to assign their PIN);
- Access number: the unique customer number that is necessary to gain access to the various services (counter, cash machines, Easy Banking Web, Easy Banking Phone, Easy Banking App, etc.) that the Bank places at their disposal.
- PIN: personal and confidential number used for identification purposes;
- Easy Banking Phone PIN: PIN that enables the holder to identify himself to get access to the Easy Banking Phone service, as well as to all other Easy Banking Phone services requiring a secured session. In accordance with the stipulations of Article IV.2, this PIN code may also, if necessary, be used when the customer contacts an adviser at the Bank for the purpose of identification, if this is required;
- CARD STOP: company appointed by the Bank to be notified in the event of loss or theft or the risk of improper use of a card;
- Device: any device which allows the holder to connect to the Internet (computer, tablet, smartphone...)
- Identification and/or signature procedures: electronic identification and/or signature techniques, more specifically:
  - card and PIN linked to the card in relation to the services Cash Withdrawal at our ATMs and paying in shops (POS) home and abroad, Cash Withdrawal at other ATMs, Self, statement printer, Cash deposit;
  - Access number and PIN for the Easy Banking Phone service;
  - electronic identification and/or signature systems provided by or accepted by the Bank that enable the holder, depending on the options provided by the Bank, to identify himself as part of the access procedure to the Easy Banking Web services, to approve and/or to sign certain orders and applications transmitted while using this service;
- Security SMS: security application that the bank may activate, consisting of a single-use code, sent by SMS to the holder's mobile, which the latter enters in addition to the electronic signature procedures made available.
- outside payment terminal: payment terminal located near the pumps outside a service station, which can only be used for paying for fuel with a card;

- Zoomit: service which enables the holder of Easy Banking Web, to view electronic documents (such as invoices, pay slips,...) which are made available to him, by the sender.
- itsme Services
    - itsme Application: mobile application provided by Belgian Mobile ID SA (registered office at Place Sainte Gudule 5, 1000 Brussels, BCE/KBO no. 0541.659.084). Depending on the options provided by the Bank, 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/or 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. TERMS OF ACCESS TO THE SERVICES AND ACCOUNTS – PROVISION OF MEANS OF ACCESS

III.1. Initial code, choosing the PIN code, delivery of the card and activation

III.1.1. The initial code

When ordering a new named card the cardholder receives an initial code. This initial code provides the cardholder with access to the secure telephone line that the Bank places at his/her disposal in order:

- that they may choose their own PIN code prior to physical delivery of the card.
- to activate their card after the physical delivery of the card.

III.1.2 Choosing the PIN code

When ordering the card, the cardholder has the opportunity to:

- select the PIN code themselves via the secure phone line placed at their disposal. Access to this line is only possible by using the initial code that the cardholder receives when ordering the card;
- have the Bank send this on a paper medium. In this case the secret code is generated by a secure application.

The cardholder may, at a later date, then change their PIN code at any time using cash machines in Belgium that are set up for this purpose.

III.1.3 Delivery of the card

Unless otherwise expressly requested by the customer, and subject to the stipulations below, the named card will be sent to the correspondence address last provided by the customer. The card is blocked when it is sent and cannot be used until the cardholder activates it by means of the secure phone line that the Bank makes available.

As an exception to the above, the named card will be sent to the customer's legal address when, at the time of contacting the Bank, the customer was identified remotely; this rule shall apply until such time as the customer has been identified in person at a branch.

III.1.4 Activation

If the cardholder has received their PIN in a letter from the Bank, the cardholder must activate their card using the secure telephone line provided by the Bank. In order to gain access to this line, the account holder is asked to enter their initial code.

If the cardholder has chosen their own PIN using the secure telephone line, the cardholder can immediately use the card, without prior activation, in shops (but not on the internet) and at cash machines.

Should the named card be issued as a result of replacement of his/her card (and without associated changes to the PIN code) or on the initiative of the Bank in relation to expiry of the card or other such reason, the activation of the card occurs on the first use of the card using the existing PIN code of the replaced or renewed card.

A temporary card may be used immediately using the PIN code that was issued at the same time as the card.

III.1.5. First use of the card

First use of the card

- must be a transaction using the PIN at a shop, at a cash machine (requesting a balance is enough) or by accessing Easy Banking Web/Easy Banking App.
- It cannot be an online payment.

III.2. The services Cash Withdrawal at our ATMs and paying in shops (POS) home and abroad, Cash Withdrawal at other ATMs, Self, statement printer, Cash deposit

III.2.1. Terms of access to the services and accounts

Subject to the provisions of this Article, one or more of the services described in Article IV below may be activated on the card, at the holder's choice. Activation applies without prejudice to other means of evidence as express confirmation of cognisance and acceptance of the rules applicable to the services, as amended from time to time; customers may request of copy of the relevant rules on durable medium at any time.

III.2.1.1. The services Cash Withdrawal at our ATMs and paying in shops (POS) home and abroad, Cash Withdrawal at other ATMs

The card holder has access to a current account for transactions carried out with the card as part of the Cash Withdrawal at our ATMs and paying in shops (POS) home and abroad, Cash Withdrawal at other ATMs. This must be a current account of which the cardholder is (co-)holder, or for which he is an authorised user or authorised card user.

A maximum of one single Cash Withdrawal service at our ATMs and paying in shops (POS) home and abroad, and one Cash Withdrawal service at other ATMs may be linked to a Welcome Pack-account if the holder is less than eighteen years of age.

The "Cash withdrawal at our cash machines", "Cash withdrawal from other cash machines" and payment to retailers" services are automatically linked to each bank card.

III.2.1.2. Cash deposit

The Cash Deposit service is activated by the card holder by using the service for the first time. For depositing euro bank notes via Cash Deposit, the card holder has access to a current account or a savings account of which he is (co-)holder or for which he is an authorised user or authorised card user.

The Cash Deposit service is not accessible to cardholders who were identified remotely when they contacted the Bank; this rule shall apply until such time as they have been identified in person at a branch.

III.2.1.3. Self services

The Self services on the card are automatically activated when the Cash Withdrawal service at our ATMs and paying in shops (POS) home and abroad is activated.

The Bank provides cards without chips, which only enable holders to use the statement service, for (an) account(s) other than the Hello Current account(s).

The holder may opt for either the basic Self service, subject to express application to this effect, or the standard Self service.

The holder may only use the Self services to carry out transactions on an account that are compatible with the scope of their powers to use the account in question.

III.2.1.3.1. Basic Self service

The card holder has access to a current account for transactions carried out using the card as part of the basic Self service. This must be a current account of which the cardholder is (co-)holder, or for which he is an authorised user or authorised card user.

III.2.1.3.2. Standard Self service

For financial transactions carried out using the card as part of the standard Self service, the cardholder has access to the following accounts:

a) a current account of which he is a (co-)holder, or for which he is an authorised user or authorised card user
b) all current and savings accounts, other than those stipulated under a), of which he is (co-)holder
c) all current and savings accounts opened to the name of a person for whom they are the legal representative.

Whenever they carry out a transaction as part of the standard Self service, holders may consult the list of accounts to which they have access on the terminal screen. The list is constantly updated to take account of events that affect the status of these accounts or the card holder's position in relation to these accounts.

Under the Self services, the holder has access to certain services to which they have subscribed and certain contracts they have concluded with the Bank, a subsidiary of the Bank or a company that is a member of the group of which the Bank is part.

III.2.1.3.3 Supplementary Self services

The Bank is entitled, but not obliged, to market new or supplementary services at any time (e.g. mobile phone services) or link new or supplementary services to the basic Self service, the standard Self and the accounts accessible under the service, in accordance with Article IV.4.

III.2.2. Signing the card upon receipt

Upon receipt, the holder must immediately sign the signature strip on the back of the card with indelible ink.

III.2.3. Use of the card and PIN

III.2.3.1. Use of the card and PIN – basic rule

Subject to the provisions of III.2.3.2. and III.2.3.3. of this Article, in order to carry out any transaction with the card, the holder must insert the card in the reader and enter the PIN on the terminal keypad.

When a cash dispenser abroad requires the holder to enter a PIN with more than four digits, the holder keys in the four digit PIN and, if required, then confirms this by selecting the relevant option.

Holders shall be notified of the approval of terminals by any appropriate means. The bank card gives access to the terminals in the Fortis Bank Self spaces and the ATMs and payment terminals with the 'Bancontact', 'Maestro', 'Cirrus', 'EC' or 'Eufiserv' logos.

III.2.3.2. Using the card and the PIN code – contactless payments

On payment terminals in some countries, the holder is not required to enter their PIN, but rather to sign a slip printed by the terminal.

In any event, for reasons of security and to guarantee the correct functioning of the card, the holder must have carried out a transaction on a Belgian ATM which requires entering the PIN.

On certain payment terminals (parking, road tolls, automatic vending machines), transactions are carried out by simply introducing the card into the terminal, followed by confirmation using the "OK" button (or not). By confirming using the "OK" button, the holder is assumed to have given their agreement to the transaction.

On some terminals (that accept contactless payments) it is possible to make payments by holding the card close to the terminal that supports this technology.

The maximum value for transactions where the PIN is not used (with or without contact) is EUR 25 per transaction and EUR 50 total value.
Exception per transaction:
- car parks: EUR 50 (Maestro)
- road tolls: EUR 100 (Maestro)

The customer therefore has to enter their PIN if these limits are exceeded.

III.2.3.3. Restrictions on use of bank card

Owing to safety considerations the Bank can impose some restrictions on the functionalities of bank cards in certain non-European countries. Therefore, the holder may not be able to withdraw cash or make payments with the card in those countries or he/she will only be able to do so under certain circumstances (e.g. only when the PIN is provided). Additional information about any restrictions of use which may apply in those countries can be provided to the customer on request. More information is available via a branch, customer service or the Bank's websites www.bnpparibasfortis.be and www.hellobank.be.

III.2.4. Entering incorrect PINs

The card is disabled if three successive incorrect PINs are entered. Holders who have forgotten their PIN should request the Bank to issue a new PIN.

III.3. Easy Banking Phone service

III.3.1. Terms of access to the accounts

The subscriber has access to the following accounts for financial transactions carried out using the Easy Banking Phone service:

via voice response computer:
- the current accounts, of which the subscriber is (co-) holder or of which he is an authorised user;
- all savings account of which the subscriber is (co-)holder or an authorised user;

through a bank adviser:
- all accounts of which he is (co-)holder;
- all accounts of which he is usufructuary. In that case, the subscriber to the Easy Banking Phone service is only authorised to carry out the following transactions: balance and transaction enquiries;
- all accounts for which he is authorised;
- all accounts opened to the name of a person who is legally represented by him.

Easy Banking Phone subscribers may only carry out account transactions that are compatible with the scope of their powers to use the accounts in question.

III.3.2. Use of Easy Banking Phone

The holder dials the access number or the account number and enters the Easy Banking Phone PIN provided by the Bank. When using Easy Banking Phone for the first time:
- via voice response computer: the holder is asked to change the Easy Banking Phone PIN provided by the Bank to a PIN of his choice;

- through a bank advisor: the holder is requested, if necessary, to identify himself with the Easy Banking Phone PIN code he received. The holder will be requested to replace the Easy Banking Phone PIN they received with an Easy Banking Phone PIN code of their own choice.

The holder may use Easy Banking Phone to change the Easy Banking Phone PIN. Easy Banking Web subscribers may also use Easy Banking Web to change the Easy Banking Phone PIN.

By subscribing to the Easy Banking Phone service via Easy Banking Web, the holder is asked to choose and initialise the Easy Banking Phone PIN.

III.3.3. Entering incorrect PINs

Easy Banking Phone is disabled if three successive incorrect PINs are entered. Holders who have forgotten their Easy Banking Phone PIN may request a new PIN from their branch or via Easy Banking Web.

III.4. Easy Banking Web service

Access to and use of Easy Banking Web is only permitted via the Bank's dedicated websites.

III.4.1. Terms of access to the accounts

The holder has access to the following accounts for financial transactions carried out using the Easy Banking Web service:

- all accounts of which he is (co-)holder;
- all accounts of which he is usufructuary. In that case, the subscriber to the Easy Banking Web service is only authorised to carry out the following transactions: balance and account enquiries on the accounts concerned, and receipt of account statements;
- all accounts for which he is authorised;
- all accounts opened to the name of a person who is legally represented by him.

Whenever they carry out a transaction using the Easy Banking Web service, holders may consult the list of accounts to which they have access on the terminal screen. The list is constantly updated to take account of events that affect the status of these accounts or the card holder's position in relation to these accounts.

Subscribers to the Easy Banking Web service may only carry out account transactions that are compatible with the scope of their powers to use the accounts in question.

III.4.2. Use of Easy Banking Web

III.4.2.1. Using the identification and/or signature procedures provided by the Bank

The Bank provides the holder with a personal card reader when the application for the service is made. The service is activated by means of initial usage.

To identify themselves or to sign orders issued or transactions to be executed using the Easy Banking Web service, subscribers use the identification and/or signature procedures provided by the Bank. They must comply with the instructions and information given in the manuals and technical appendices.

III.4.2.2. Using the itsme Application and 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- of 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 Easy Banking App 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 by the Bank for this purpose.

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.

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

III.5. PIN security

The PINs provided by the Bank are calculated and printed by computer in accordance with very strict security procedures.

With regard to the PIN code chosen by the cardholder themselves over the phone, the Bank takes the necessary precautions to ensure:

- the procedure is extremely secure;
- the confidentiality of the self-selected PIN code is guaranteed.

The Bank takes all the necessary measures to ensure the secrecy of the PINs used as part of the services.

III.6. Third-party payment applications

The Bank allows the Cardholder to link her or his card to certain third-party payment applications through which she or he may initiate payment transactions based on that card (initiating these payments using Bancontact and/or Maestro depends on the options selected in the application concerned to make use of Bancontact and/or Maestro)..
Specific transaction limits may apply. The Cardholder must accept the terms and conditions and the privacy policy set out by the editor of the relevant payment application, which editor distributes such application under its exclusive responsibility. The Bank is not a party to the agreement between the Cardholder and the editor of the relevant payment application.
The Cardholder's obligations and liabilities as set out in article VII of these Terms and Conditions, especially in respect of security, of confidentiality and of notification of lost or stolen card or of any risk of unauthorized use of the card or of the PIN Code, fully apply to the Cardholder in the context of using a third-party payment application. In this context, the word "card" used in these Terms and Conditions includes any device containing the third-party payment application, including as the case may be the Cardholder's mobile phone; the word "PIN Code" includes the security means of the third-party payment application and/or of the device containing that application.

IV. DESCRIPTION OF SERVICES

IV.1. Services linked to a bank card

IV.1.1. Cash withdrawal at our ATMs and payments in shops (POS) home and abroad

This service is automatically linked to every bank card. This service offers card holders the possibility to withdraw cash at our ATMs and to pay purchases of goods or services to third parties who use payment terminals home and abroad (with the Bancontact or Maestro logo and subject to the provisions of Article III.2.3.3)). This service is charged as soon as the card is assigned as provided for in the price list referred to in Article X.2.

When paying by card at an outdoor terminal in a petrol station, given that the exact payment amount is not known in advance, a certain fixed amount is reserved during the period strictly necessary for filling with fuel on the initiative of the oil company. The exact amount of the fuel you take will be deducted from the amount available for your card payments after filling up with fuel. The balance of the reserved amount will then be released.

IV.1.2. Cash withdrawal at other ATMs

This service is automatically linked to every bank card.
This service offers the possibility to withdraw cash at ATMs of banks other than BNP Paribas Fortis and Fintro in Belgium and at all ATMs abroad (subject to the provisions of Article III.2.3.3. These ATMs display the logos of 'Bancontact', 'Maestro', 'Cirrus', 'EC' or 'Eufiserv'.
This service is activated by means of initial usage.

IV.1.3. Balance enquiries

The balances of your accounts can only be consulted in Belgium at BNP Paribas and Fintro ATMs and the other banks which are equipped to this end. In principle, the balances shown are the balances at the end of the last bank business day prior to the day of the enquiry.

IV.1.4. Changing the PIN

This service is only available in Belgium. Holders may change their PIN to a new PIN of their choice at cash dispensers displaying the Bancontact logo, at Self terminals, and also at some terminals in the Bank branches.

IV.1.5. Remote payments

Holders may transmit an order for payment by card to a trader or third party as part of a remote agreement.

The Bank may take all and any measures aimed at preventing holders using their card for a payment as part of a remote agreement without electronic identification.

Holders who are also subscribers to Easy Banking Web or holders of a card reader may, when they wish to use their card for payment under a remote agreement made with a trader over the Internet, first be requested to identify themselves and sign for the payment, using the electronic signature procedures made available by the Bank, in particular under the Easy Banking Web service, in accordance with Article IV.3, paragraph 3.

IV.1.6. Bank card with photo

Holders of cards other than Hello Bank cards have the option to personalise their bank cards by applying a photo on the front of the card through intervention of the Bank. Cardholders can choose a photo of themselves or a picture from the gallery made available by the Bank for this purpose. The stipulations of the Photo Card are included in the 'Rules concerning the bank card with photo'. These rules are available on the Bank's website www.bnpparibasfortis.be and can be requested at the Bank branches.

IV.1.7. Specific transactions at the BNP Paribas Fortis Self terminals

IV.1.7.1. Transfers

Transfer orders may be entered on Self terminals of BNP Paribas Fortis.

IV.1.7.2. Printing account statements

Statements issued by BNP Paribas Fortis Self terminals are original statements. If several cards are linked to one and the same account, statements are delivered to the first holder to enter his card in the machine.

If card holders do not withdraw statements from statement printers within a period of ninety days, the statements shall be printed and sent to the account holder's correspondence address. In this case postal charges shall be paid by the account holder.

Holders of a card that entitles them to obtain account statements from BNP Paribas Fortis Self terminals may request that no further statements are sent by post; in that case, they undertake to collect their statements from BNP Paribas Fortis Self terminals as frequently as possible.

Should the cardholder request account statements using the Self terminal and there are more than 99 pages to be printed, this process will not proceed. In such a case the account statements will be printed and forwarded by post. In this case postal charges shall be paid by the account holder.

The statement printing service does not enable the printing of statements for the Hello Current account.

IV.1.7.3. Cash deposit

Subject to the restriction mentioned in Article III.2.1.2, the card holder has the possibility to deposit euro bank notes on an account at the Bank through specially equipped ATMs.

Bank notes can be deposited via Self Cash for:

- accounts of which the customer is holder or co-holder;
- accounts for which the customer is legal representative of the holder;
- the reference account of the card if the card holder is an authorised user.

The card holder deposits the bank notes in the specific module of the Self Cash deposit machine. This can be done in several stacks. The card holder has to confirm the amount counted by the machine. If the card holder does not agree with the count of a stack, he can interrupt the transaction and all the bank notes in the stack will be returned (except suspicious and false bank notes). The card holder receives a ticket specifying the detail of the deposit for the stack(s) he confirmed. After confirming the deposited amount, the account selected by the card holder will be credited.

The Bank has the possibility to enter limits per transaction, per card and per account for the deposits.

A specific and unique electronic verification is carried out on every bank note deposited in the Self Cash deposit. Without prejudice to the evidence to the contrary by the customer, the verification by the Bank provides evidence of the recorded transaction during which a bank note was deposited.

Unrecognisable notes are returned to the customer through the module without crediting the account.

False bank notes are withheld by the machine without crediting the account.

IV.2. Easy Banking Phone

The Easy Banking Phone service enables the holder to use a touch-tone phone to link up with the Bank's voice response computer to make account enquiries, obtain information on banking and insurance products, make transfers, and purchase and manage certain financial or other services marketed by the Bank, in accordance with the procedure stipulated in Article IV.4.

Holders can also contact a bank adviser via Easy Banking Phone (by identifying themselves by means of their access number and their Easy Banking Phone PIN code, either at the start of the telephone conversation, or during the course of it) for the purposes listed in the first paragraph, and to carry out investment transactions, transmit orders and requests, and obtain general financial information and personalised information and advice according to the 'Easy Banking Phone' stipulations provided in article IV.4.2. All telephone conversations are recorded by the Bank.

IV.3. Easy Banking Web

a) Features

The Easy Banking Web service enables holders to use a device to link up with the Bank's computer to, in line with the available features on the Bank's website that the holder is accessing, make account enquiries, obtain information on financial and insurance products, carry out transfers and investment transactions, transmit orders and requests, electronically sign data by means of a signature created according to the terms and exhibiting the characteristics referred to in Article IV.3 (b) below, use the Zoomit service, obtain general banking information and personalised information and advice, exchange messages with the Bank, and purchase and manage certain financial or other services marketed by the Bank, in accordance with the procedure stipulated in Article IV.4.

b) Electronic signature of data

The Bank, on the site(s) and for the type(s) of data that it determines, may ask the holder to create an electronic signature that identifies him or her and that is uniquely associated with him or her. The signature guarantees the integrity of signed electronic data. This signing procedure is exclusively for use in the context of relations between the Bank and the holder, to the exclusion of any other use.

The signature is created under the control of the holder. To this end, the holder authorises the Bank, for the electronic data that it presents to him or her on the screen (for example the file containing data relating to an instruction or to the subscription to a service by the holder), to create or have created an electronic signature certificate identifying the holder and to create his or her electronic signature by means of the certificate. The certificate is subject to the terms and conditions of use specified in the Bank's certificate management policy available on the Bank's website and provided when the request is made to authorise the creation of each certificate. The holder accepts these terms and conditions of use by authorising the creation of the certificate.

The holder grants this authorisation by means of the signing procedure specified by the Bank. The procedures and steps involved in creating the electronic signature are specified on the screen.

The Bank sends the holder an electronic document containing the electronic data, bearing the holder's electronic signature which the holder can then check. The signed electronic document is intended exclusively for use in the context of relations between the Bank and the holder, to the exclusion of any other use.

c) Security SMS

For the prevention of fraud or any other abuse, the Bank reserves the right to activate the "Security SMS" application defined in Article II for the services and features that it determines, under the conditions and according to the terms it shall advise. The holder must comply with the instructions and information given via the service in question.

d) Miscellaneous

The Easy Banking Web service also enables holders to contact a Bank advisor for the purposes of assistance with the service (Easy Banking Web Helpdesk); all telephone conversations are recorded by the Bank.

Holders using an Internet connection and with a card on which the "Cash withdrawal at our ATMs and paying in shops (POS) home and abroad" service has been activated may use the card to pay for purchases from a shopkeeper using a remote sales system on an Internet site; the holder identifies themselves and signs the transaction by means of the electronic signature procedures made available by the Bank in particular as part of the Easy Banking Web service.

The Bank informs the holder of the technical features and configuration required for the device used in order to enable the services to function correctly. This information is available on the Easy Banking Web screens.

IV.4. Purchase and management of financial services as part of Self banking, Easy Banking Phone and Easy Banking Web

Holders may use the Self banking, Easy Banking Phone and Easy Banking Web services to purchase, amend and cancel certain financial and other services marketed by the Bank. Holders use fully or partly electronic transactions to enter requests to purchase, amend or terminate the services referred to above.

IV.4.1. Fully electronic transactions

Fully electronic transactions work as follows:

- With the Self and Easy Banking Web services, holders can select the transaction on the standard menu screen. With the Easy Banking Phone service, the transaction may be activated by pressing a key or combination of keys.
- Once all details of the request have been given, the holder signs the request by means of the specific signature procedure for the service he uses.
- Once signed by the holder, the entire request is routed and processed electronically.
- If the request is entered using the Self and Easy Banking Web services, the holder is informed at once – unless the transaction is interrupted due to a technical incident – of the outcome of his request (accepted, refused or subject to examination by the Bank).
- The Bank provides the holder with confirmation that his request has been accepted and provides the requisite information by means of an advice sent with the account statement, by ordinary mail or by any other electronic mail system.
- In cases where the request concerns services that the Bank operates commercially for other entities, acceptance of the request can, if required, immediately be confirmed by the entity in question.

IV.4.2. Partly electronic transactions

In the context of the Easy Banking Web service:

A partial electronic transaction is carried out as follows:

-
- The holder sends a request electronically.
- Once the request data have been completed, the holder signs the request by means of the specific signature procedure that he uses for this service.

The Bank provides the holder with confirmation of the outcome of their request (accepted, refused or subject to examination by the Bank) and provides the requisite information by means of an advice sent with the account statement, by ordinary mail or by any other electronic mail system. In cases where the request concerns services that the Bank operates commercially for other entities, the Cardholder can, if required, immediately be informed of the outcome of their request by the entity in question.

In the context of the Easy Banking Phone service

A partial electronic transaction is carried out as follows:

Holders submit a request to the bank adviser by telephone.
After the request has been processed, the Bank provides the Cardholder with confirmation of the outcome of their request (accepted, refused or subject to examination by the Bank) and provides all necessary information by means of a message sent with the account statement, by ordinary mail or by any other electronic mail system. In cases where the request concerns services that the Bank operates commercially for other entities, the Cardholder can, if required, immediately be informed of the outcome of their request by the entity in question.

IV.4.3. List of transactions available for the purchase, modification and cancellation of commercialised financial services

- For PC banking the list of available transactions can be consulted via the PC banking service. The holder of this service can also be informed about possible transactions via personal messages sent to him as part of this service. The content of the services provided can evolve, in the understanding that certain services can be added, changed or cancelled by the Bank.
- For the Phone banking service the holder of this service can be informed about the available transactions via an adviser of the Bank.
- The available transactions for the Self service can be consulted on the menu of this service.

V. LIMITS

V.1. Cash withdrawals – payments on payment terminals

V.1.1. General rules

The following limits are the standard limits for use in relation to the cards.
The total of cash withdrawals is 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

The total of payments in shops (POS) home and abroad, as well as remote payments are limited to a maximum of EUR 2,500 per card per seven-day period.

The card holder has the possibility, in the course of the agreement, to increase or reduce the standard limits within the limits of the Bank's offer below. The limits for cash withdrawals and payments can be adjusted by mutual agreement. The increase of the limits can be subject to prior agreement of the Bank. The standard limits for cash withdrawals may not be increased by cardholders who were identified remotely when they contacted the Bank, until such time as they have been identified in person at a branch.
Cardholders also have the option of temporarily adjusting their payment limits (for a period of 1 to 7 days), using the channels made available by the Bank, for exceptional withdrawals or payments.
In such cases account is only taken of these limits during the limited period. Temporary limit changes for exceptional cash withdrawals are not authorised for cardholders who were identified remotely when they contacted the Bank, until such time as they have been identified in person at a branch.

In the context of the battle against fraud, the Bank reserves the right to automatically and with immediate effect reduce card limits, if necessary, for certain retailers or specific activity sectors, when:
-the card holder fails to respect the obligations arising from the current General Terms and Conditions
-the Bank's fraud detection systems indicate potential fraud on the account(s) to which the holder has access or linked to this/these account(s).
-the conditions applied by the Bank to the provision of a certain limit are no longer being fulfilled during the course of a later inspection.

Cash withdrawals

per card/day	per card/7 consecutive days
EUR 25	EUR 25
EUR 30	EUR 50
EUR 40	EUR 80
EUR 50	EUR 125
EUR 125	EUR 250
EUR 250	EUR 500
EUR 250	EUR 1,250
EUR 500	EUR 1,250
EUR 625	EUR 1,250
EUR 625	EUR 2,500
EUR 1,250	EUR 5,000
EUR 2,500	EUR 5,000
EUR 4,500	EUR 5,000
EUR 7,000	EUR 7,500

Payment to retailers (per card/per 7 consecutive days)

EUR 25
EUR 50
EUR 80
EUR 125
EUR 250
EUR 750
EUR 1,250
EUR 2,500
EUR 5,000

The total of cash withdrawals and payments in shops (POS) home and abroad, as well as distance payments may not exceed EUR 9,990 per account per seven-day period.

Cash withdrawals at ATMs may, depending upon the owner of the ATM, be limited to lower amounts than the amounts mentioned above.

V.1.2. Rules applicable to Welcome Pack (holders aged under 18)

The rules given in this Article apply to Welcome Pack of which the holders are below the age of 18.
The following limits are the standard limits for use in relation to the cards.

The following limits apply for cash withdrawals:

- Maximum amount per card and per day (midnight to midnight):
  EUR 125
- Maximum amount per card per 7-day period: EUR 250

The total of payments in shops (POS) home and abroad, as well as remote payments are limited to a maximum of EUR 250 per card and per 7-day period.

On explicit request of the legal representative standard limits can be increased or reduced within the limits of the offer below:

Cash withdrawals

per card/day	per card/per 7 consecutive days
EUR 25	EUR 25
EUR 30	EUR 50
EUR 40	EUR 80
EUR 50	EUR 125
EUR 125	EUR 250
EUR 250	EUR 500
EUR 250	EUR 750

Payments to retailers (per card/per 7 consecutive days)

EUR 25
EUR 50
EUR 80
EUR 125
EUR 250
EUR 500
EUR 1,250

V.2. Transfers

Under this Article, a transfer in favour of a third party is deemed to be any transfer to an account not accessible to the holder as part of the services, i.e. an account other than those mentioned in Article III.2.1.3.2, Article III.3.1 or Article III.4.1 of these General Terms and Conditions.

The following global limits apply for all transfers entered by Easy Banking Phone and on Self terminals: transfers from a current account to a savings account and vice versa are limited to the available balance on the account to be debited; transfers from a current account to a third party are limited to the available balance on the account to be debited, with an upper limit of EUR 5,000 per day and up to EUR 10,000 per week.

The sending and/or receipt of international transfers (beyond the Single Euro Payments Area and the European Economic Area) is not authorised from or to an account whose (joint) holder(s), or one of them, was identified remotely when they contacted the Bank, until such time as they have been identified in person at a branch.

Transfers in favour of third parties made by Easy Banking Web are limited to a maximum of EUR 300,000 per account per day. However, the Bank reserves the right to limit this maximum amount to an amount to be determined by the Bank in the event of the risk of fraud or similar abuse.

Under the Easy Banking Phone and Self services, transfers from a Welcome Pack (the holder of which is under 18) to a third party are limited to the balance available on the account to be debited, with an upper limit of EUR 625 per day and EUR 1,250 per week. The same limits apply for the Easy Banking Web service.

V.3. Transactions involving financial instruments

Purchase and sale of financial instruments (including shares, units in investment funds and bonds) via Easy Banking Web are subject to a limit of EUR 250,000 per transaction.

VI. OBLIGATIONS AND LIABILITY OF THE HOLDER

VI.1. Basic obligations – safekeeping of cards, PINs and signature procedures

The holder is obliged to use the services in accordance with the terms and conditions governing the issue and use thereof.

The holder must make sure that he performs his transactions direct via the special banking services described above. In particular, access to and use of Easy Banking Web or use of identification and/or signature procedures (made available by the Bank as part of the Easy Banking Web service) must take place exclusively via the Bank's dedicated website.

Cards, PINs, including the itsme Code and identification and signature procedures are strictly personal to the holder.

The holder shall take all the precautions required to ensure the safekeeping of their card, PIN and identification and signature procedures and shall, if appropriate, keep them secret. Holders undertake to memorise their PIN, including the itsme Code, not to write it on any document, object or support whatsoever, and not to divulge or reveal it in any way. They likewise undertake not to leave their card, PIN or signature procedures where they can be seen by third parties, and not to make the card, PIN, itsme Code or signature procedures available to third parties.

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

VI.2. Notification of loss or theft and any risk of fraudulent use of cards, devices, PINs and signature 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.

Cardholders shall notify the lost and stolen card help line (CARD STOP) immediately when they become aware of the loss or theft of their card or the risk of fraudulent use of the card.

Subscribers to an online banking service shall notify the Easy Banking Web Helpdesk immediately when they become aware of the loss or theft of their electronic identification and signature procedures and/or his device, or the risk of fraudulent use thereof.

If the electronic identification and signature device for Easy Banking Web involves the use of a card and reader, the subscriber shall notify CARD STOP immediately when they become aware of the loss or theft of the card or the risk of the fraudulent use thereof.

CARD STOP can be contacted round the clock on 070 344 344. CARD STOP records all telephone calls.

The Easy Banking Web Helpdesk is only available on certain days and at certain times. Subscribers may obtain information on the Easy Banking Web Helpdesk opening hours from their branch or on the Bank's website www.bnpparibasfortis.be.

If holders become aware of loss, theft or fraudulent use outside of Easy Banking Web Helpdesk opening hours, they shall notify the Helpdesk immediately when the service is accessible again or as soon as reasonably possible.

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.be or, during its opening hours, through 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 site.

CARD STOP, the Easy Banking Web Helpdesk or the itsme Helpdesk, as the case may be, shall immediately provide the holder with a file reference number serving as proof that notification has taken place.

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

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

Holders must check, as frequently as possible, the status of accounts linked to the transactions carried out using the services and transactions recorded on the accounts.

If the holder ascertains that a payment transaction is unauthorized or has not been duly executed, they shall proceed in accordance with the instructions given under "Payment Services" in the Bank's General Terms and Conditions.

VI.4. Liability for improper use of cards, PINs and signature procedures

VI.4.1. Up until the time of notification

Until the time of the notification stipulated in Article VI.2.,holders are liable for the consequences of the loss or theft of their card or signature procedures, up to an amount of EUR 150, other than in the event of gross negligence or fraud, in which case this limit does not apply. The aforementioned maximum amount does not apply in the case of use for professional purposes.

VI.4.2. After notification

Once the notification as stipulated in article VI.2. has been made, holders are no longer liable for the consequences of the loss or theft of their card or signature procedures, unless the Bank can prove that the holder has acted fraudulently, and subject to the provisions of Article VI.4.3.

VI.4.3. Gross negligence

VI.4.3.1. General

Depending on the actual circumstances and without prejudice to the judge's sovereign powers to judge, gross negligence may arise if the holder:

- failing to notify, as relevant, CARD STOP, or the Bank or Belgian Mobile ID in the case of online banking services, of the loss, theft or any risk of abuse of their card, equipment or identification or signature procedures, as soon as they become aware of it;
- failing to check regularly, the status of accounts linked to the transactions carried out using the services and individual transactions recorded on the accounts, and this results in a delay in the holder becoming aware of the fraudulent use of the card, and/or of their identification and signature procedures and duly notifying the Bank;
- failing to take the precautionary measures provided in Article VI.6.;
- failing to provide notification of the loss or the theft of their card, their device or signature procedures to the police authorities in the area where the loss or theft occurred within 24 hours of becoming aware of events.

VI.4.3.2. Failure to honour precautions in respect of PINs including the itsme Code and signature procedures

VI.4.3.2.1. Fraudulent use of PIN, itsme Code and identification and signature procedures

Subject to the limitations set out above, the following is understood to be gross negligence on the part of the holder:

- writing down the PIN/itsme Code in a readable form on the card, the device or on an object or document that the holder kept or carried together with the card;
- disclosing the PIN/itsme Code to a third party;
- store the personal security features together with the card reader, give or reveal them to a third party.

There is no gross negligence on the part of the holder if the PIN is obtained by extortion, either with actual violence against the holder, their property or one of their immediate relatives or with the threat of violence against the holder, their property or one of their immediate relatives.

VI.4.3.2.2. Failure to honour precautions in respect of a card

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

The holder shall not be liable for gross negligence, if:

- the theft of the card involves violence against their person, property or relatives or if there is the threat of violence to the holder's person, property or relatives;
- the card is stolen from their place of residence as specified below. The following are not considered as the principal residence: any second home and any holiday home owned by the holder or account holder, and any student lodgings. The theft must involve breaking and entering, cat burglary, violence, threats or skeleton keys. Depending on the circumstances and without prejudice to the judge's sovereign powers to judge, gross negligence may arise if the card is left anywhere other than the place of residence, where the holder stays occasionally or temporarily (for instance, a hotel room, hospital room, tent, camper, caravan, motor home, mobile home or boat), unless the card has been deposited in a safe that the owner or the manager of the establishment provides for customers or in a locked drawer or cabinet.

Within the above restrictions, leaving the card unattended can be considered gross negligence:

- at the place of employment, unless the card is in a locked drawer or cabinet
- in a vehicle, locked or unlocked, even if it is parked in a private driveway
- in a public place or a place accessible to the public, unless the card is in a locked drawer or cabinet
- on private premises (including the place of residence) to which several people besides the holder have access, such as for receptions, parties (including family parties), conferences, screenings, exhibitions, sports activities or competitions, unless the card is kept in a locked drawer or cabinet
- in courtyards, entrances and gardens that are private property
- in the common parts of a building subject to co-ownership agreements.

VI.4.3.3. Other cases of gross negligence

Within the scope of the above restrictions, gross negligence of the holder may be enabling the people listed below to use the card, device, PIN/itsme Code, identification and signature procedures or personal security features fraudulently as a result of failure to take adequate precautions or exercise due diligence with regard to the card, PIN or signature procedures:

- the holder, co-holder or authorised user of an account which is linked to the transactions carried out using the services;
- the spouse, cohabiting partner, guests or visitors (for private or professional reasons) of the holder or of the accountholder;
- people, employed or not and irrespective of their status, who work for, or are employees of, the holder or of the account holder;
- parents and relatives of the holder or of the account holder.

VI.5. Execution and irrevocable nature of orders sent using the services

Holders may not revoke an instruction to transfer funds issued by means of a card or sent using an online banking service once it has been received by the Bank.

However, if the cash transfer was to be executed on a date agreed with the Bank, it may be revoked up until the day preceding the agreed execution date.
The holder shall provide the Bank with written, signed notice of the revocation. For transfers executed under the Easy Banking Web service, transfer orders with a specified date or execution date may be revoked electronically by using the "Delete" function. The revocation order is signed using the signature procedures provided by the Bank.

The account holder irrevocably authorises the Bank to debit their account with the amount of transactions carried out with a card. Any unauthorised overdraft resulting from such debit shall not in any way constitute the granting of a credit facility, and the account holder shall settle the amounts concerned immediately.

Payment instructions sent using the services shall be carried out by the Bank provided that the account status and the agreements that governs the account so permit.

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

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

VI.6. Precautionary advice

The Bank recommends that the holder take the precautionary measures with respect to the use of the services as stipulated in this Article.

VI.6.1. Precautionary measures regarding the card

Sign all new cards immediately upon receipt.

Keep your card on you or in a safe place.

Never leave your card unattended at your place of work. An increasing number of cards are being stolen from places of work.

Never leave your card unattended in public places or places which are accessible to the public or in private premises where other people are present, unless the card is in a locked drawer or cupboard.

Never leave your card in your vehicle, even if it is parked in your private driveway.

Keep your payment slips and cash withdrawal vouchers.

Place a stop order on your card immediately if it is withheld by a cash dispenser for no valid reason.

Withdraw your statements from Self terminals, subject to what is stated in Article IV.1.8.2 or download them via Easy Banking Web on a regular basis. Always check your statements as soon as you receive them. Notify the Bank immediately of any error or inaccuracy.

VI.6.2. Precautionary measures regarding the PIN including the itsme Code

Memorise your PIN as soon as you receive it, and then destroy the document on which the PIN was sent by the Bank.

When you receive the PIN for your card, change it at a cash dispenser as soon as possible.

As soon as you receive your Easy Banking Phone PIN, log into the Easy Banking Phone service using a voice-activated computer, and choose the PIN you want to use in future for Easy Banking Phone.

Your PIN/itsme Code must remain secret: do not disclose them to anyone, not even a member of your family, a friend or a person that you consider reliable.

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

Never write your PIN/itsme Code down, even in coded form, e.g. by hiding it in a false telephone number.

Always enter your PIN/itsme Code away from prying eyes, whether at a cash dispenser, in a shop or on the keyboard of your device. Never allow anyone to watch and always ensure that you cannot be seen without your knowledge (hide the keypad with your hand). Do not let anyone distract your attention or have an unknown person help you. If you notice anything out of the ordinary, inform the Bank and, if necessary, the shopkeeper, immediately.

When selecting a new PIN, avoid combinations that are too obvious (e.g., part of your date of birth, your telephone number, your post code, etc). Choosing the same PIN for all your cards and access codes may seem like an easy way out, but this is obviously risky.

If you have reason to believe that someone else knows your Easy Banking Phone PIN, change it immediately using option 1-4-1 under the Easy Banking Phone service "Changing personal details" If it is no longer possible to access the Easy Banking Phone service with your PIN, call Fortis Bank Customer Service on the number mentioned on the websites of the Bank www.bnpparibasfortis.be or www.hellobank.be.

In the same way, if the confidentiality of your itsme Code is compromised, change it immediately or block your itsme Account using the channels provided by Belgian Mobile ID.

VI.6.3. Precautionary measure regarding the Easy Banking Web service

Make sure that you only access and use Easy Banking Web or identification and/or signature procedures provided by the Bank as part of this service via one of the Bank's dedicated websites.

Do not leave your device unattended during an Easy Banking Web session. Close the program using the "Log out" button as soon as you are no longer using the Easy Banking Web service. Make sure that the device you use is secured against viruses, spyware and adware by means of the necessary software such as anti-virus and firewall software and make sure they are always up-to-date. Some viruses can take control of your device, thus causing security risks, not only in relation to online banking, but to all software, files or functions on your device.

VI.7. Online banking services: right of use and intellectual property

Holders have a strictly personal right to use software provided by the Bank as part of the services. This software is the property of the Bank and/or persons that have assigned the operating rights to the Bank.
It is strictly forbidden for any other party to use, call up or share this software as part of, or from, another Internet application or software program – to extract data via Easy Banking Web or execute transactions, for instance.

The design of the Easy Banking Web websites, the texts, graphics and other components of this are the property of the Bank and must under no circumstances be altered, reproduced or distributed without the Bank's prior written consent.

VII. THE BANK'S OBLIGATIONS AND LIABILITY

VII.1. Period of validity of the card

The card has a fixed period of validity. The card will automatically be renewed on the expiry date, except in case of refusal by the Bank or cancellation by the holder, notified to the Bank one month before that expiry date.

In case of loss, theft or technical faults with the card, other than a Hello Bank card, the cardholder can, in expectation of receiving a new named card, obtain a temporary card from the Bank's branches.
The services, functions and limits of the temporary card are the same as for the named card it is temporarily replacing.
Use of the temporary card is limited to 3 months after its date of issue.

VII.2. Posting of the card, PIN code and initial code

The Bank bears the risk for all items posted to the cardholder for the card, the PIN code or the initial code.

VII.3. Internal transaction log

The Bank shall keep an internal log of transactions carried out with the card using the services for a period of ten years as from 1 January in the year following the date on which the transactions were carried out.

VII.4. Amendment to card limits

The Bank will change the card limits on request of the holder within the limits and conditions specified under V.1.1. and V.1.2.

The Bank agrees to lower the limit at the request of the holder in any of the following circumstances: if the card or PIN is lost or stolen, or if their account statements include any transactions carried out without their approval.

The cardholder also has the capability to temporarily change the limits (for a period of 1 day to 1 month) for exceptional cash withdrawals or payments. In such cases account is only taken of these limits for the limited period. This option is not available to cardholders who were identified remotely when they contacted the Bank, until such time as they have been identified in person at a branch.

The Bank reserves the right to refuse any request for an increase in the limit without providing the grounds for its decision.

VII.5. Proof of transactions carried out using the services

The essential data for all electronic transfers made using the services is recorded and stored by the Bank in such a way that it can be reproduced in legible form on any type of medium. In the event of any dispute with the holder regarding one of these transactions, and without prejudice to evidence to the contrary furnished by the holder, provided that the latter is acting as a consumer, the Bank shall refer to this data to demonstrate that the transaction was duly recorded and booked and was not affected by any technical incident or other malfunction.

Some cash dispensers and payment terminals provide – at the express request of the holder, or automatically – a voucher giving the transaction reference and amount. This voucher is provided without prejudice to the provisions of the first paragraph of this Article.

VII.6. Continuity of online banking services

The Bank shall use its best endeavours in designing and developing programs and software for access to online banking services. The Bank shall do all in its power to ensure continuity of the services and 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 terminals or new versions of the software, provided that such suspension is limited to a reasonable period of time.

VII.7. Failure to execute transactions – erroneous execution of transactions – transactions carried out without authorisation – forgery

Without prejudice to the obligations and liability of the holder set forth in Article VI and subject to the provisions of Article III.2.3.3, the Bank is liable for:

- the failure to execute, or the erroneous execution of, transactions carried out using the services, involving machines, terminals or equipment 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 errors or irregularities in management of the services that are attributable to the Bank;
- the use of counterfeit cards in the event of third parties forging the card;
- the risk for every transmission to the holder of a card or of every means that allows the use thereof.

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

- when, as a result of failure to execute, or incorrect execution of, the transaction, there is a loss equal to all or part of the amount of the transaction, with the amount of such loss plus, in applicable, interest;
- with the amount that may be required to return the holder's situation to what it was prior to the unauthorised transaction, plus interest on this amount, if applicable;
- with the amount required to return the holder's situation to what it was prior to use of a counterfeit card;
- with the amount of any other financial loss or charges, including charges paid by the holder to determine the amount for which compensation is payable;

In respect of the online banking services, the Bank does not accept any liability whatsoever for any loss whatsoever, 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.8. Provision of 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.

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 transpiring to be inaccurate or for the way in which holders might interpret or use the information provided.

VIII. PROOF IN RESPECT OF ONLINE BANKING

VIII.1 Identification and/or signature procedures

In addition to the Standard Terms and Conditions, in particular Article 22 thereof, the subscriber explicitly 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 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 procedures constitutes, for both the account holder and the Bank, proof of identity, of his or her agreement 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 should they claim there was an error or irregularity.

VIII.2 Recordings

Recordings of telephone calls as provided for under Articles IV.2. and IV.3. are subject to the provisions of Article 9 of The Bank's General Terms and Conditions, relating to recording and processing personal data. The Bank keeps recordings for ten years, after which they 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 entries constitute full proof of the content of the telephone conversation, including for orders and/or requests made by the holder. In the event of dispute, they may be produced as evidence before the body appointed to resolve the dispute.

In cases where telephone conversations concern services the Bank operates commercially for other entities, the Bank may pass on the recordings made of the telephone conversations to the entity in question for the purposes stated above.

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

The Bank reserves the right, when it deems useful or necessary, to ask the holder to confirm telephone orders and/or requests by means of letter, fax, e-mail or any other electronic message system. The Bank may postpone the execution of orders pending receipt of such confirmation.

Fax copies, printed e-mail messages and messages sent by any other electronic message system shall be deemed to be written documents, and shall have the same evidential value as original documents.
Any loss or damage arising from fraud or error in respect of orders and requests confirmed by fax, e-mail or any other electronic message system shall be borne by the holder, unless the holder produces evidence of fraud or gross negligence on the part of the Bank.

The Bank reserves the right to postpone the execution of orders or requests confirmed by fax, e-mail or any other electronic message system if it is of the opinion that such orders are not sufficiently authentic, and to request a paper order or substantiating documents.

As part of the services, the holder may send the bank orders and/or requests by e-mail or any other electronic message system. The procedures set out in paragraphs 5, 6 and 7 of this Article in respect of evidential value and the liability of the holder and of the Bank also apply to messages sent by such means.

IX. TERM OF THE AGREEMENT AND TERMINATION OF THE SERVICE

This agreement is made for an indefinite period.

The holder may terminate the agreement, free of charge, at any time subject to one month's notice.

The Bank may terminate the agreement at any time subject to two months' notice, or subject to one month's notice in the case of use for professional purposes.

However, the Bank may terminate the service with immediate effect if the holder fails to honour one of his obligations towards the Bank, or if the Bank becomes aware off acts that jeopardise the relationship of trust and confidence between the holder and the Bank.

The Bank reserves the right to instruct the network of cash dispensers and payment terminals in Belgium or abroad and traders, to withhold a card, or refuse transactions with a card, and the right to suspend the holder's access to the online banking services if:

- several incorrect PINs are entered in succession;
- the card is defective or damaged;
- the card was left in the terminal by mistake;
- the holder uses the card or service in a way that is contrary to these General Terms and Conditions;
- the holder fails to honour one of his obligations towards the Bank, or the Bank becomes aware of facts that jeopardise the relationship of trust and confidence between the 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.

X. CHARGES FOR SERVICES

X.1. Subscription fees for the services

The services are provided subject, where applicable, to a periodic subscription fee that is automatically debited from the current account to which the services give access. The Easy Banking Phone service is free.

X.2. Other charges

The following are or may be subject to charges:

- management fee bank card;
- all transactions carried out using the services;
- fund transfers and payments made pursuant to orders transmitted using the services;
- provision of a new card;
- provision of a new PIN;
- sending the SMS code associated with the signature as part of the Security SMS service.;
- replacement of a part of the electronic identification and signature device under the Easy Banking Web service and Security SMS;
- amendment to the limit for the card;
- replacing a lost or stolen card;
- providing a bank card with photo;
- provision of a temporary card.

Costs for transactions (cash withdrawals/payments to retailers) do not include any charges that certain retailers or ATM providers may apply.

Cash withdrawals and payments made using a card in a currency other than the euro shall be converted at the exchange rate determined on the basis of the indicative exchange rates published by the European Central Bank plus an exchange margin which is stated in the list of rates and charges. The exchange rate is that which applies on the day the Bank receives the instruction.

Subscribers to the Easy Banking Phone or Easy Banking Web service shall be liable for:

- the costs of acquiring, installing and running the terminal, computer equipment or other electronic identification and signature device that enables them to access the services
- costs for connecting to the Internet or other networks
- the telecommunications costs as part of the Easy Banking Phone and Easy Banking Web services.

X.3. Information about the rates, debit or credit date and value dates

Please refer to the "Payment Services" General Banking Terms and Conditions and the list of charges, which are available to the holder in all the Bank branches and on the Bank's websites www.bnpparibasfortis.be or www.hellobank.be.

XI. COMPLAINTS AND RECOURSE

Complaints may be sent to the Bank via the customer's branch, via Customer Service or using the complaint form available via Easy Banking Web or on the Bank's Internet site.

If the customer is not satisfied with the proposed solution, they may submit their complaint in writing to the following address:

Complaints,
Montagne du Parc 3,
1000 Brussels.

If the customer is not satisfied with the solution proposed by the Bank, they may, in their capacity as a natural person acting for private purposes, submit the complaint to the Ombudsfin – Ombudsman in financial conflicts, either by ordinary mail at the address below, or using the complaint form available on the Internet site:

Ombudsfin – Ombudsman in financial conflicts
North Gate II
Boulevard du Roi Albert II 8, box 2
1000 Brussels
Fax: +32 2 545 77 79
E-mail: ombudsman@ombudsfin.be - www.ombudsfin.be

In addition, if the complaint concerns a payment service, it may be submitted in writing to the General Management, Supervision and Mediation, of the FPS Economy, SMEs, Independent Professions and Energy, WTC III, Boulevard Simon Bolivar/Simon Bolivarlaan 30, 1000 Brussels.

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.

XII. AMENDMENTS TO THESE GENERAL TERMS AND CONDITIONS

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

When sending the information mentioned in the first paragraph, the Bank shall also advise holders 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.

Appendix 1 to the General Terms and Conditions of bank cards and the Easy Banking Phone and Easy Banking Web services. Terms and conditions of the Zoomit service available via Easy Banking Web.

1. Purpose of the Zoomit terms and conditions

The purpose of the terms and conditions of the Zoomit service (hereinafter referred to as the "Terms and Conditions") is to describe the Isabel Zoomit service as offered by the Bank as part of its Easy Banking Web service and to set out the rights and obligations associated with this service.

2. Definitions

2.1 Unless specified or stated otherwise in these Terms and Conditions, the definitions included in Article II of the General Terms and Conditions of bank cards and the Easy Banking Phone and Easy Banking Web services also apply to these Terms and Conditions.

2.2 In addition to those definitions, the following definitions are also used in these Terms and Conditions.
The "Document": refers to any electronic document, whether or not it contains financial data (including, but not restricted to, invoices, credit notes and wage slips) made available to one or more Addressees by a Sender using Zoomit.
The "Contracting Party" or "You": any private individual who has entered into a Easy Banking Web contract and hence has the Zoomit function.
The "Addressee": refers to the private individual or legal entity, bona fide organisation or government body that is a customer of the Sender to which Documents are sent via Zoomit. If appropriate, the Addressee stipulates which Users may access the Documents via their Easy Banking Web application.
The "User": the Contracting Party who, as a subscriber to the Easy Banking Web service, has access to Documents via the Zoomit function, either as an Addressee or as a person authorised by the Addressee to access the Documents.
The "Sender": refers to an entity which issues Documents of which it is the official holder and makes them available to one or more Addressees via Zoomit, in accordance with the relevant agreement entered into with Isabel.
"Isabel": Isabel SA/NV, with its registered office at Boulevard de l'Impératrice/Keizerinlaan 13/15, B-1000 Brussels, Belgium, Register of Companies 0455 530 509, the company used by the Bank to provide Zoomit.
"Access code": refers to the unique, confidential reference of a commercial and/or non-sensitive Document that may be issued by the Sender and sent to the relevant Addressee to obtain access to the Document (for example, on the paper invoice), as described in more detail in the Zoomit product specifications.
"Zoomit": refers to the Isabel service that enables Senders to make Documents available to Addressees securely, and enables Addressees and/or Users to recover, consult, save and manage documents and pay securely by means of their Easy Banking Web application.

3. Description of Zoomit

With Zoomit, the Addressee or User may consult all kinds of Documents made available by various Senders, completely securely and free of charge. Access to these documents is obtained through the Easy Banking Web application.
Zoomit also facilitates payment of any invoices made accessible to Users via the Documents made available through the Easy Banking Web service offered by the Bank. Zoomit is not, however, a payment function *per se: payments are made solely via and by the Bank without any involvement by Zoomit.*
For the execution and processing of Zoomit, the Bank uses Isabel, acting as the Bank's processor. The Bank and Isabel act only as a mailbox for the Documents transmitted between the Addressees and Senders, adding a secure link to the Document (as notified by the Senders) to the corresponding Addressee's bank account(s).
The Bank and Isabel shall exchange other additional information on the relative status of the Document (for instance, concerning a payment transaction performed or to be performed in the case of an invoice). However, the information exchanged is not selected or amended by the Bank or Isabel, but merely sent to the Addressee stipulated by the Sender.

Unless contractually agreed otherwise, the electronic signature of Users, shall be binding on the Addressee, both vis-à-vis Isabel and vis-à-vis other Senders, in the same way as a handwritten signature.
Senders are entitled to include advertising material in the Documents, provided that such material relates only to information on the Senders' own products and services.
For further details of the technical features of Zoomit, Users should consult the website: www.zoomit.be.

4. Access to Zoomit

4.1 Any subscription to or membership of the Easy Banking Web service implies subscription to or membership of the Zoomit service and acceptance of these Terms and Conditions, which form an integral part of the General Terms and Conditions of bank cards and the Easy Banking Phone and Easy Banking Web services.

4.2 All Senders have entered into a "Sender" agreement with Isabel so that the Addressees and Users can consult Documents using the Bank's Zoomit service.

4.3 In addition to the contractual framework with the Bank, a specific authorisation must be given, via Easy Banking Web, for each Sender and each type of Document before actual access to the Documents from that Sender takes effect.
However, it may be that a Sender obtains such agreement from an Addressee, independently of the Easy Banking Web service, so that the Documents are directly accessible in Zoomit for that Addressee and Users, via Easy Banking Web, without any other formality. In that case, the Sender shall have sole liability for obtaining this authorisation, with the Bank and Isabel only assuming responsibility for communicating what they receive from the Sender.
The User authorises the Bank and Isabel, as the processor, to provide notice of the availability of Documents in Zoomit before the User itself has added this Sender to its list of Senders.

4.4 Other than in the event of a serious or deliberate mistake on its part, the Bank does not accept any liability regarding the contractual relationship between Isabel and the Sender and between the Addressee and the Sender.

4.5 The User shall be required to comply with these Terms and Conditions, and with the guidelines provided with regard to this service.
The Addressee has sole responsibility for managing these Zoomit access rights. Any loss or damage ensuing from fraud or unauthorised access to the Documents that is due to inadequate or inappropriate management of these rights shall be borne by the Addressee, except in the event of a serious or deliberate mistake on the part of Isabel and/or the Bank.
Only Addressees and Users that confirm receipt of authorisation from the Addressee shall be entitled to access a Document via Zoomit. If a User other than the Addressee erroneously receives an access right to a Document for which the Addressee has not granted the User such right, he/she shall not open it and shall notify the Addressee and/or the Sender of this error immediately.
Further information on the operation of Zoomit is available online (www.zoomit.be).

5. Provision of Documents

The Addressee or the User shall have access to the Document from a Sender after a consistency test has shown, in accordance with Article 10, that he/she is actually authorised to consult this Document.
By clicking on the Document, the User leaves the Easy Banking Web application and is redirected, via a secure link, to the

server of the Sender or a specified third party he/she has designated, where the User can consult the Document, without this document being stored on the Bank's or Isabel's systems or servers.

Unless otherwise agreed with the Sender, all links to a Document via Zoomit will be made available for a period of at least 18 (eighteen) months (the "Availability Period"), starting from the time the Zoomit network becomes aware of the Document location and the Addressee's identity.
The Addressee acknowledges and accepts, both on their own behalf and for Users, that:

- the Addressee may download and store any Document, at the Addressee's discretion and under the Addressee's responsibility, during the Availability Period;
- Documents are no longer available upon expiry of the Availability Period or upon termination of the contractual relationship between the Addressee and Sender or if all or some of the Senders' and/or Addressee's Zoomit service is cancelled for any reason;
- the fact that Documents are made available by Zoomit may, according to the contractual arrangements with the Sender, result in it no longer being possible to send all or some of the Documents via another channel (for instance, only a copy by ordinary mail, fax or e-mail, or a copy of the Document via Zoomit). This is at the Sender's sole responsibility. The Bank and Isabel accept no liability in this regard, other than in the event of a serious or deliberate mistake on their part.
- neither the Bank nor Isabel accepts any liability whatsoever concerning the content of sites/servers to which they create or authorise a link, and do not provide any guarantee as to the level of security of such sites. This is the Sender's sole responsibility.
- neither the Bank nor Isabel provides any guarantee as to the solvency and/or reliability of Senders, site owners or holders, or concerning the persons or companies on which these sites/servers provide information.
- If the Bank so provides, the Documents that show the payment status "to pay" (or similar) may be paid directly in Easy Banking Web. Once the payment or direct debit order has been issued by the Addressee, the Document status will be changed by the Sender to "payment initiated" (or similar) or "payment made" (or similar).
- The Document status does not refer to execution of a payment and cannot therefore be used as proof of payment (only bank statements can be used as proof). The Addressee acknowledges that there is no link between the payment and the status as given in Zoomit.

6. Cancellation and closure of the Zoomit service

6.1 Either the User or the Bank may cancel the Zoomit service as detailed below.

6.2 Since the Zoomit service is an integral part of the Easy Banking Web service, the User may only cancel the Zoomit service totally subject to and in accordance with the same conditions as for cancellation of the Easy Banking Web service.

6.3 Using the Zoomit management module, the Addressee may terminate the provision of Documents via the Zoomit service by some or all Senders at any time, free of charge. Unless the Sender's terms and conditions stipulate a different cancellation deadline, specific cancellation of this kind takes effect on the following business day. Unless stated to the contrary in these Terms and Conditions, the Sender is no longer obliged, after cancellation, to again provide Documents that have already been made available via Zoomit by any other means.
In the event of cancellation of the Easy Banking Web service or in the case referred to in paragraph 1 above, the Addressee undertakes to notify the Senders concerned as soon as possible and to agree new arrangements with them regarding the provision of Documents.

6.4 Subject to the following, the Bank may, subject to two months' notice, terminate the Zoomit service or the provision of Documents via the Zoomit service for some or all Senders.

In addition, the Bank may, at any time and without prior notice, terminate the Zoomit service or suspend all or some of the execution thereof if the User is in serious breach of their commitments towards the Bank, including failure to honour the security procedures and any unauthorised access or attempted access to Zoomit and/or to Documents.

7. Interruptions to Zoomit

Isabel and the Bank reserve the right to suspend the Zoomit service for maintenance or to modify or improve the system. The Bank will inform You of this in advance to the extent possible. However, it may be that the Bank is unable to notify You of certain interruptions due to a technical incident or an event of force majeure, including but not restricted to strikes or any other event beyond the Bank's control, or in the event of a serious emergency.

8. Liability

The Bank or Isabel cannot guarantee that Zoomit will be compatible with the User's own requirements and wishes, in particular regarding their computer and telecommunication system.
Without prejudice to the following, and other than in the event of fraud or a serious mistake, neither the Bank nor Isabel is liable for:

- the Zoomit service being unavailable due to maintenance works, scheduled or otherwise, or due to faults or an event of force majeure;
- access errors or inability to access Documents via Zoomit, if this results directly or indirectly from incorrect or incomplete information sent to the Bank or to a Sender;
- the User acting, or failing to act, in a way that is contrary to a clause of these Terms or Conditions or any legislation or regulatory or contractual clause that applies to its relationship with its own customers;
- the User failing to honour the security instructions and/or guidelines;
- failure of the consistency test when the Addressee sends incorrect or incomplete data to the Bank or the Sender;
- the impossibility of making any connection needed to ensure the performance of the service, or interruptions to such connection, in any way whatsoever, if this is attributable to third parties;
- any direct or indirect financial, commercial or other loss or damage, such as loss of time, loss of customers or harm to customers, loss of data, loss of revenue, loss of earnings, increase in general expenses, disruption of business activities, legal action by third parties, loss of reputation or projected savings that derive from or are associated with use of Zoomit.

If the Bank and/or Isabel is/are held liable and required to compensate for loss or damage, this liability shall in all cases be limited to compensation for proven direct loss or damage. The overall liability of the Bank and/or Isabel as regards Zoomit shall be limited to EUR 25,000, regardless of the gravity of the error. Neither the Bank nor Isabel is liable for the content, or the accuracy and availability of Documents exchanged by means of Zoomit. The Bank does not, therefore, deal with complaints or queries regarding these Documents or the content thereof and any complaints or queries should be sent directly to the Senders.

9. Data Protection

Use of Zoomit entails the processing of personal data as defined in the Act of 8 December 1992 on personal data protection (Data Protection Act). Depending on the Document concerned, this personal data may in particular include the surname, first name, assumed name, e-mail address, bank identification number or bank account number of the Sender, Addressee and/or User, as well as any other personal data that the User

has provided to the Bank or Sender or has authorised the Bank and/or Sender to collect.
You accept that the Bank and its processor may process this personal data, the data sent to the Senders and/or additional data that You enter in the Zoomit application to manage access to and the provision of Documents to the Addressee and Users and to ensure the due operation of Zoomit.
You therefore authorise the Bank and Isabel to notify You of the availability of Documents, if appropriate even without adding the Sender to the list of Senders authorised to make Documents available via Zoomit.
You also accept that the Bank and its processors may use the aforementioned personal data in an integrated form for the purposes of statistics and reports.
In practice, access to Documents and making them available in particular implies processing of the following data:

- As a user of the Easy Banking Web service, you accept that the Bank and/or its processor (Isabel) exchange identity details of the Addressee and/or Users with potential and/or existing Senders, provided that this is required for sending and providing Documents. Only identity details that are correspondingly required for these purposes are exchanged (at this stage, this involves the surname, first name, postal address, e-mail address, bank account number and knowing whether or not the Addressee uses Easy Banking Web and/or Zoomit).
- The Bank then enables the Addressee, using the Zoomit button, to see, for each bank account number for which there are Documents, whether it is possible to access these Documents. An invoice is always attached to a payment transaction;
- Depending on the case, the Bank is authorised, based on this processing, to add a Sender to your list of Senders or to save (via its processors, if appropriate) your agreement to the Sender's terms and conditions to be able to add a particular Sender to your list of Senders;
- A consistency test is conducted, provided by the Bank and the Sender to Isabel, which is responsible for processing the data, in accordance with Article 9.

During the processing of this personal data as part of Zoomit, all the parties concerned shall comply strictly with the rules imposed by the Data Protection Act. For this purpose, the Sender acts as the party responsible for the processing of personal data as part of its contractual relationship with You to enable You to send Documents electronically and to consult them. As the processor, the Bank is responsible for processing your personal data to enable You and the Users to consult Documents using Zoomit.
You have the right, vis-à-vis the relevant data processor, to consult your data and have it amended free of charge. You may avail yourself of these rights by writing to the relevant data processor.
The Bank and its processor (Isabel) take all the measures and use all the security techniques (adding a key, etc.) required to protect the personal data they process – including the link to the Document, but excluding the Documents themselves (which are the responsibility of the Sender) – against loss, theft, damage and unauthorised access. The User's personal data is not shared with third parties that are not involved in the management and operation of Zoomit.

10. Consistency test

Running the consistency test is a best efforts obligation from Isabel. This means that as a processor of the Sender and the Bank, Isabel will compare the identity details of the Addressee and/or their Users, as known to the Bank, with those received from the Sender.
There are several options concerning the Document sensitivity:

1. If the Document sensitivity is set as "commercial document", the consistency test assumes consistency between the identity of the Addressee and/or authorised User (surname, first name and aliases) and the Addressee's bank account number, as specified by the Sender, and the same items as specified by the Bank. If the first test fails (for instance, because another User accesses the Document), a second consistency test is run to compare the Contracting Party's unique company number, as provided by the Sender, with the number as known to the Bank. If this second consistency test fails, it is still possible to access the Document by means of the corresponding Access Code.
2. If the Document sensitivity is set as "non-sensitive", the consistency test assumes consistency between the identity of the Addressee and/or authorised User (surname, first name and aliases) and the Addressee's bank account number, as specified by the Sender, and the same items as specified by the Bank. If the consistency test fails, it is still possible to access the Document, as appropriate, by means of the corresponding Access Code or if the User accessing the Document has been so authorised by the Addressee. The Addressee is notified and may still object to this if required.
3. If the Document sensitivity is set as "sensitive", the consistency test assumes consistency between the identity of the Addressee and/or authorised User (surname, first name and aliases) and the Addressee's bank account number, as specified by the Sender, and the same items as specified by the Bank. If the consistency test fails, access to the Document is refused.

The Sender alone decides on the sensitivity option appropriate to the Documents. The Addressee shall arrange with the Sender if it is necessary to change this sensitivity option.

11. Intellectual property rights

The property and other intellectual rights associated with the Zoomit service, such as rights on programmes, software, databases, protected graphic designs and interfaces, as well as brands, commercial names and logos, remain the property of their respective owners. You shall refrain from breaching such rights.
Throughout the subscription to Zoomit, You have a non-exclusive, non-transferable personal licence enabling You to use Isabel's Zoomit computer programmes in accordance with the agreed object, in particular for making Documents available.
You are only authorised to use the Zoomit application, the documentation relating thereto and other protected items associated with this application on your own behalf as part of use of this function.
You are not authorised to make any copy of these items, distribute them or use them other than as associated with use of this application as part of the Easy Banking Web service, or to change any item whatsoever of the Zoomit application.