These Visa CyberCard General Terms and Conditions enter into force on 1 January 2018.
The use of the Visa Cyber Card is governed by the following terms and conditions:

1. Definitions

The terms set out below are defined as follows for the purposes of these General Terms and Conditions:

- Bank: ING Luxembourg, Société Anonyme of which particulars are given below, acting in the capacity of card-issuer and, where applicable, lender;
- Card: any Cyber Visa Card, whether primary (= card issued in the name of a card account-holder) or additional (= card issued in the name of any other person than the primary card account-holder);
- Visa CyberCard: a credit card issued by Visa;
- Card account: the account to which transactions, conducted using the card, are recorded;
- Cardholder: refers to any or all of the individuals (natural and legal) in whose name or names a card is issued and who is/are authorised to use it or each individually;
- Primary card account-holder: refers to all of the card account-holders, or each individually; all of the primary cardholders being jointly and severally liable;
- Bank working day: a bank working day such as defined in the Bank's tariff in force;
- Consumer: a natural person who, in relation to payment service contracts with the Bank, acts for a purpose other than that of his commercial or professional activity;
- Exceeding of agreed limit: a tacitly accepted overdraft in accordance with which the Bank grants the cardholder, under the responsibility of the primary card account-holder, access to funds in excess of the balance on the card account;
- 3D Secure: an internationally recognised standard of cardholder identification for online credit card payments which is called "Verified by Visa" when paying with Visa. Its purpose is to increase the security of online transactions by reducing the potential for fraud.
- www.ing.lu: web address allowing access to the Bank's website on the international Internet network;

2. Entry into effect of services

2.1. To obtain a card it is first necessary to make a card application to the Bank.

The Bank reserves the right to issue a card without having to justify its decision.

2.2. The Bank is authorised to refuse the card application if the primary card account-holder provides incomplete or erroneous information, notably with regard to his financial position. Moreover, the desired overdraft facility indicated in the card application by the primary card account-holder may be reduced by the Bank in view of the primary card account-holder's financial position. The primary card account-holder shall be informed thereof by post or email.
2.3. (Clause applicable only to the primary consumer card account-holder of a personal card).
The primary card account-holder and the cardholder expressly declare that they have been informed that the contract relating to the card application will take affect after the card is used for the first time and no later than fourteen calendar days after the signature of the card application by the primary card account-holder and the cardholder. They therefore retain the right to withdraw their card application until the entry into force of the contract by returning the card to the Bank as appropriate. After this point the primary card account-holder and the cardholder shall be deemed to have read, understood and accepted the card application, the Bank's General Terms and Conditions, the Bank's tariff and these General Terms and Conditions Visa CyberCard.

3. Issue of additional cards

3.1. At the request of the primary card account-holder, the Bank may issue an additional card to any person designated by the primary card account-holder and approved by the Bank.
As a result, the primary card account-holder authorises the cardholder to withdraw funds from the card account.
3.2. When an additional card is issued, the primary card account-holder and the cardholder are jointly and severally liable for all claims arising from the use of said additional card.
3.3. The Bank reserves the right to revoke an additional card at any time, notably at the written request of the primary card account-holder or following the cardholder's relinquishment of the card and whenever the provisions of article 13 below authorise it to do so in the various manners described therein. In such a case, the primary card account-holder will remain jointly and severally liable with the cardholder in question for any transactions made using said card until such time as the card is returned.

4. Description of the services provided

4.1. The card may be used to pay for goods and services purchased online (and to make any other type of payment accepted in the Visa Network by simply quoting the card number) with greater security than a standard Visa card. In order to limit the risk of fraudulent use associated with the circulation of the card number, the card does not take the form of a physical plastic card. The credit limit on the card is that detailed in article 10 below.
The card is simply a Visa number and a Card Verification Value (CVV2 - a code required by certain internet sites).
Since the card has no physical form, it cannot be used to make cash withdrawals from automatic teller machines or to make payments at point-of-sale terminals.
4.2. Transactions made using the card are debited from or credited to the card account and have the same status as cash transactions.
4.3. Unless otherwise agreed, any credit to an account for a transaction, for which settlement is not known or not final at the time of input, is made “subject to completion”, even when “subject to completion” is not expressly mentioned. If the transaction is not actually completed or if the wrong amount is credited, the Bank is expressly authorised to automatically debit the corresponding amount to the account without notice.

5. Card use

5.1. The cardholder shall use the card only when the account contains sufficient funds and in accordance with his credit limit.
5.2. In order to pay for goods and services purchased online, the cardholder must enter their Visa card number following the instructions provided by the relevant internet site, in some cases together with the Card Verification Value (CVV2) if required by the relevant internet site.
5.3. Any payment transaction made using the card in one of the manners described above shall be deemed to have been authorised by the primary card account-holder and the cardholder.
5.4. The Bank is thereby expressly authorised to debit the card-account with the amount of these transactions as recorded by the Visa service electronic systems under the card number.
5.5. Any instruction, of any kind, given using the card is irrevocable once approved by the cardholder.
5.6. Use of the card shall be deemed to constitute express acceptance of the conditions in force applicable to the card.
5.7. When a payment transaction is initiated by or through the payee as part of a card-related payment transaction and the amount is unknown at such time when the cardholder authorises the payment transaction, the Bank reserves the right to block funds available on the card account.

6. Proof of transactions

6.1. Any transaction made via the Visa service using the card number shall be deemed to have been made by the cardholder and only the cardholder.

6.2. Evidence that a transaction has been made and completed correctly is provided by the Bank in the form of the records kept by the Bank and/or the Visa Network.

6.3. The primary card account-holder and the cardholder accept the fact that these records constitute formal and sufficient evidence that the relevant transactions have been authorised by the cardholder.

7. Security regulations

7.1. Both the Visa card number and the corresponding Card Verification Value (CVV2) are strictly personal and non-transferable.
7.2. Upon receipt the cardholder is bound to take all necessary steps to ensure their protection; they agree:

- To memorise them or keep them in a safe place not accessible to third parties
- Not to give them to any third parties (except when making a payment transaction).

Failure to observe these security instructions shall be deemed to constitute gross negligence and shall render both the primary card account-holder and the cardholder liable to bear the totality of any loss resulting from the fraudulent use of the card until such time as it is reported in accordance with article 8 below.
7.3. The primary card account-holder and the cardholder accept and acknowledge that preventive procedures authorised by the Visa network may be put in place in order to avoid potential fraudulent use, notably in the case of businesses known or suspected by Visa to be fraudulent or from risky countries. These procedures may result in the blocking of some or all of the card's functions. Under no circumstances shall the Bank be held liable in such a situation.

7.4. Terms and conditions of use of the 3D Secure service

7.4.1. Purpose

3D Secure is an internationally recognised standard of cardholder identification for online credit card payments. It is called "Verified by Visa" when paying with Visa. Its purpose is to increase the security of online transactions. The primary card account-holder and/or the account-holder can immediately check on the merchant's website if they have chosen to secure payments via the 3D Secure standard.
The 3D Secure service Terms and Conditions of use define the procedures for the latest version of 3D Secure technology (replacing the static 3D Secure version).

7.4.2. Activation of the 3D Secure service

7.4.2.1. The primary card account-holder and/or cardholder can activate 3D Secure via the Internet Banking Service of the Bank or via a portal dedicated to 3D Secure.

a) Activation via Bank Internet Access

The primary card account-holder and/or the cardholder must activate 3D Secure by registering their card according to the procedure defined by the Bank.

b) Activation via the dedicated portal:

In order to activate 3D Secure for their Visa card, the primary card account-holder or cardholder must request an activation code (single-use registration code) via the dedicated portal https://3dsecure.lu The activation code will be sent by post to the primary card account-holder at the address they provided to the Bank for correspondence by mail.
The primary card account-holder and/or the cardholder can activate 3D Secure on the dedicated portal with the activation code. For this purpose, the primary card account-holder and/or the cardholder must follow the activation procedure which requires entering the activation code.
7.4.2.2. During activation, the primary card account-holder and/or the cardholder must select at least one of the identification methods below to proceed with the execution of a transaction on the Internet requiring 3D Secure identification (hereinafter the "3D Secure transaction"):

a) Validation of the 3D Secure transaction with a Token-type LuxTrust certificate (hereinafter the "LuxTrust certificate":

In order to link the LuxTrust certificate to their card, the primary card account-holder and/or the cardholder must enter their LuxTrust user-id, their LuxTrust password and the one-time password provided by the LuxTrust certificate during the activation procedure.

b) Validation of the 3D Secure transaction using a single-use code provided by SMS:

In order to link their card to their mobile telephone, the primary card account-holder and/or the cardholder must provide their telephone number during the activation procedure. If activation of the 3D Secure service is requested via the dedicated portal, the issuing Bank will send a single-use registration code by SMS to the telephone number provided by the primary card account-holder and/or the cardholder via the intermediary of a service provider specialised in sending SMS-type messages. The primary card account-holder and/or the cardholder must enter the single-use code to finalise activation of the 3D Secure service.
7.4.2.3. The primary card account-holder and/or the cardholder must also set up a personal security message. The personal security message will appear on all 3D Secure transactions.
7.4.2.4. Activation of the 3D Secure service is free and takes place over an encrypted Internet connection. Activation of 3D Secure by the primary card account-holder and/or the cardholder implies their acceptance of the Terms and Conditions CyberCard.
7.4.2.5. The primary card account-holder and/or the cardholder must activate each of their credit cards separately. If the primary card account-holder and/or the cardholder receive(s) a new credit card with a new PIN number (e.g. in the case of loss or theft), this card must also be activated.
7.4.2.6. Transactions cannot be executed with online merchants requiring 3D Secure identification if 3D Secure hasn't been activated.

7.4.3. Card use and authorisation

a) Execution of a 3D Secure transaction with a Token-type LuxTrust certificate (hereinafter the "LuxTrust certificate"):
The primary card account-holder and/or the cardholder must validate execution of 3D Secure transactions with their LuxTrust user-id, LuxTrust password and the one-time password provided on the LuxTrust certificate.

b) Execution of a 3D Secure transaction with a single-use code provided by SMS:

The primary card account-holder and/or the cardholder must validate execution of the 3D Secure transaction using the single-use code sent by SMS to the telephone number provided by the primary card account-holder and/or the cardholder, as appropriate, at the time of activation of 3D Secure for the card in question.
Entry of the security elements required (including, depending on the identification method selected, the LuxTrust user-id, LuxTrust password and one-time password provided in the LuxTrust certificate or the single-use code provided by SMS) confirms approval of the payment by card in accordance with the provisions of these Terms and Conditions Visa CyberCard.

7.4.4. Obligation of due diligence and co-operation

7.4.4.1. The primary card account-holder and/or the cardholder, as appropriate, must ensure the protection and secrecy of their security elements and of any tools or systems (credit card, LuxTrust certificate or mobile telephone) required for transaction validation.

They must not write down the security elements or save them in electronic format in either full or modified form, whether encrypted or not, or provide them to a third party.
The primary card account-holder and/or the cardholder, as appropriate, must select a personal security message when they activate the 3D Secure linked to their card.
They must not write down or save their personal security message in an electronic format, either in full or modified form, whether encrypted or not, either close to the card or elsewhere. The primary card account-holder and/or the cardholder also agree not to provide their personal security message to third parties or to make it accessible to any third parties in any way whatsoever.
7.4.4.2. At the time of 3D Secure transaction validation, the primary card account-holder and/or the cardholder must ensure that the dedicated portal includes all of the following security elements:

- The portal address begins with "https"
- The portal address bar displays a lock
- The portal displays the personal security message defined by the primary card account-holder and/or the cardholder
- The portal contains the logo "Verified by Visa".

Should any of these security elements be absent from the dedicated portal, the primary card account-holder and/or the cardholder, as appropriate, must refrain from validating the transaction. They will be solely liable for any prejudice resulting from the entry of their security elements and validation of the transaction.
7.4.4.3. In the event that one of the security elements is missing from the dedicated portal, or if fraudulent use of the security elements is suspected by the primary card account-holder and/or the cardholder, they must immediately inform the issuing Bank and block the card in accordance with the procedures described in these Visa CyberCard General Terms and Conditions.
The primary card account-holder and/or the cardholder must immediately change their personal security message if they have reason to believe that a third party has knowledge of it.

7.4.5. Processing of personal data

7.4.5.1. The primary card account-holder and/or the cardholder mandate the issuing Bank for the processing of their personal data to ensure proper functioning of the card and to prevent, detect and analyse fraudulent transactions.
7.4.5.2. In addition to the provisions covering the processing of personal data included in the Visa CyberCard General Terms and Conditions, the primary card account-holder and/or the cardholder specifically authorise(s) the Bank to send their personal data to third parties whose intervention is required for 3D Secure use, notably to the companies responsible for managing the dedicated portal and the codes required to activate the 3D Secure service, and for validating 3D Secure transactions.
Given this context, the primary card account-holder and/or the cardholder expressly acknowledge(s) that they have been informed that use of 3D Secure requires the intervention of third-party companies, notably for validation via the LuxTrust certificate and SMS, transmission of the activation code and management of the dedicated portal. The data transmitted can also be stored with these third-party companies, including in other countries.
The Bank responsible for processing personal data commits to handling the data in accordance with the legislation applicable to the protection of privacy with regard to the processing of personal data.

7.4.6. Liability

7.4.6.1. The liability clauses in these Visa Cyber Card General Terms and Conditions and in the Bank's General Terms and Conditions are valid for 3D Secure use.
The issuing Bank does not guarantee that the 3D Secure service will always be available and cannot be held liable for any damages resulting from service failures, disruptions (including for required system maintenance) or overloading of the systems of the Bank or of any of the Bank's commissioned third parties.
7.4.6.2. The Bank cannot be held liable for any 3D Secure service failures, respectively for damage resulting from a failure, malfunction or disruption of electronic communications networks (Internet, mobile telephony) or public servers, or from social conflict or any other events outside of its control.

7.4.7. Termination

7.4.7.1. The Bank reserves the right to terminate the 3D Secure service at any time.

8. Loss or theft

8.1 In the event of the loss, theft, fraudulent use of the card or if the primary card account-holder suspects that an untrustworthy third party has had access to this number, they must notify the Bank immediately by calling +(352) 49.49.94 and indicating the number of the card in question.
Until the incident is reported and without prejudice to fraudulent acts on the part of the primary card account-holder or additional cardholder, the primary card account-holder is liable for all losses suffered as a result of non-authorised payment transactions with the card until this time and unless there was fraudulent use by them or the cardholder.
The primary card account-holder and the cardholder shall be liable, within the limits established by law, for losses resulting from unauthorised payment transactions, except where the losses are the result of fraudulent actions on their part or on the part of the cardholder or of a failure to comply with the requirement of card use in accordance with the conditions governing its issue and its use, either intentionally or following gross negligence. This will also be the case if the primary card account-holder or the cardholder delays informing the Bank or the entity designated by the latter of the loss, theft or misappropriation or of any unauthorised use of the payment instrument.
The card holder alone is responsible for the safekeeping of his card number.
Its use by a third party shall be deemed to constitute proof that the card number was accessible to another person and that the cardholder failed to follow the security instructions.
The cardholder shall, however, be entitled to submit evidence to the contrary.

The cardholder shall give the Bank any information they have about the circumstances of the theft or loss. They shall provide the Bank with a copy of the declaration of loss/theft made to the relevant police authorities.
This article is without prejudice to article 3.2 of these General Terms and Conditions Visa CyberCard.

8.2. Information provided to the primary account-holder and the cardholder by the Bank in the event of suspected fraud or fraud.
The Bank makes available/provides to the primary account-holder and the cardholder the secure procedure through which the primary account-holder and the cardholder can report any suspected fraud, fraud or security threats.
This procedure is available on www.ing.lu.

9. Method of payment

9.1. Each month, the Bank shall issue a statement of the transactions made during the previous month. Unless otherwise instructed, this statement shall be addressed to the primary card account-holder.
9.2. The card offers the primary card account-holder and/or the cardholder two payment options:

- Either payment of all the transactions detailed on the statement prior to the deadline indicated thereon, in which case no commission will be charged;
- Or payment of at least the minimum amount indicated on the statement before the deadline indicated thereon, in which case the primary card account-holder shall pay a commission equal to the balance outstanding on that date multiplied by the rate detailed on the Bank's tariff in force on the date of issue of the statement.

If the minimum amount required is not paid by the deadline indicated on the statement, the Bank shall charge the primary card account-holder an additional fee as set out in the Bank's tariff in force at the time in addition to the aforementioned commission.
In such a case, the Bank also reserves the right to block the use of the card by the primary card account-holder.

10. Overdraft facility

10.1. Throughout the period of validity of the card, the cardholder shall have an overdraft facility on the card account up to the amount communicated by the bank and confirmed in the card account statement. The cardholder may use this overdraft facility at any time by overdrawing the account up to this limit against which any funds then credited to the account will be offset.
10.2. The annual rate of interest applicable to this overdraft facility is that indicated in the Bank's tariff in force at the time the card account is overdrawn. This interest is calculated over the exact number of days the account is overdrawn.
10.3. Debit interest shall be set off against any credit interest payable on the card account and charged on a quarterly basis.
10.4. Unless otherwise indicated, all guarantees provided or to be provided by or for the primary card account-holder in favour of the Bank, irrespective of the date of their provision, shall guarantee the payment or repayment of any sums owed now or in the future by the primary card account-holder under the terms and conditions set out herein.
10.5. All costs incurred by the Bank in the recovery of its debt shall be borne by the primary card account-holder.
10.6. The Bank is authorised to change the overdraft facility at any time subject to the conditions set out in article 15 of these General Terms and Conditions Visa CyberCard.

11. Validity of the card

The expiry date of the CyberCard is specified when the Visa card number and the verification value (CVV2) are issued.

12. Exclusion of liability

12.1. The Bank cannot be held liable for any indirect loss resulting from a failure of any kind in the operation of the Visa Network.
12.2. Moreover, the Bank shall not be held liable for any prejudice suffered following any network failure or any other event outside its reasonable control.
12.3 Similarly, under no circumstances shall the Bank be held liable if the card is refused by any business or internet site.

13. Termination or suspension

13.1. The card is granted for an indefinite period.

13.2. The primary card account-holder or the cardholder may terminate the contract at any time subject to one month's notice. They shall, however, remain bound to repay to the Bank any debit balance on the account, the amount of any transactions pending and any other undertakings made in respect of the Bank in relation to the use of the card.
The Bank reserves the right to charge a fee for the termination of the contract in accordance with its tariff in force at the time, except in the case of termination of the contract by a consumer after a period of twelve months.
13.3. The Bank may terminate the contract and revoke the card subject to two months' notice by notifying the primary card account-holder and the cardholder by letter or email. The termination of the contract shall legally render the total debit balance on the card account payable.
13.4. The card account shall not be closed definitely until four months after the return of the card number and/or the security number. Any credit balance on the account in question shall therefore not be repaid to the primary card account-holder until the end of this four month period. Any security attached to the card shall therefore be retained for the same period.
13.5. The Bank may also suspend all or any of the card's functions fully or in part, provisionally or once and for all, at any time and at its entire discretion for any reason relating to:

- **The security of the card and, notably to the expiration of card validity, to the closing of the card account, or in the event of transactions which appear to represent a breach of public order or decency or to have been made for illegal purposes;**
- **Any presumption that the card has been used without authorisation or fraudulently, notably at the request of the primary card account-holder and/or the cardholder, and during any fraud prevention procedures following Visa's regulations; or,**
- **Whenever the Bank notes that the solvency of the primary card account-holder and/or the cardholder is compromised, when any security obtained is insufficient or security requested has not been obtained.**
- **All applicable cases covered in the General Terms and Conditions of the Bank.**

If a card is blocked, the Bank shall inform the primary card account-holder and/or the cardholder that it has been blocked and the reasons for this by statement of account or by mail (paper or electronic), if possible before the card is blocked, or immediately thereafter unless providing this information is unacceptable for reasons of security or prohibited under any European or national legislation.
The Bank shall unblock the card or replace the card number and/or the security number as soon as the reasons for which it was blocked cease to apply.
The primary card account-holder and the cardholder shall not be entitled to claim any compensation as a result of the suspension of the card under the conditions set out in this section.
The (primary) cardholder may request unblocking of the card by contacting their local branch or telephoning +(352).49.49.94. The Bank shall be entitled to refuse the unblocking if, at its full discretion, it considers that the reasons for blocking the card persist.

14. Tariffs

14.1. The card is issued against payment of an annual fee which is deducted automatically from the card account.
The amount of this fee is set out in the Bank's tariff in force at the time.
14.2. The card account bears credit or debit interest calculated "pro rata temporis" on the basis of the account balance and in accordance with the Bank's tariff in force at the time.
14.3. In the event of currency conversion, the Bank shall debit a currency conversion charge from the account in accordance with its tariff in force at the time and in the currency of the account.
14.4. The Bank reserves the right to change the exchange rates, the debit and credit interest rates and the charges and fees relating to the card at any time according to the Bank's General Terms and Conditions in force at the time; only the primary card account-holder will be notified of this.

15. Amendments to these general terms and conditions

Without prejudice to the Bank's right to add new services at any time and to change the card or amend these General Terms and Conditions Visa CyberCard pursuant to the new legislation or regulations, the Bank may amend these General Terms and Conditions Visa CyberCard only by notifying the primary card account-holder thereof at least two months prior to their entry into force.
The existence of such amendments shall be notified to the primary card account-holder via the Bank's secure website, by written notices enclosed with bank statements or by any other (postal or electronic) correspondence sent by the Bank to the primary card account-holder. The primary card account-holder shall immediately inform any other cardholder(s) of the amendments proposed by the Bank.
If the (primary) cardholder does not wish to accept these amendments, they shall return the card to the Bank for cancellation prior to the date of entry into effect of the amendments. Unless otherwise stipulated, this termination shall be free of charge and take effect immediately.
Failure to exercise this right shall automatically be deemed to constitute acceptance of the amendments by the primary card account-holder and the cardholder. The primary card account-holder alone shall be liable for any direct or indirect losses resulting from any failure to inform the cardholder.

16. Data protection

The Bank, as data controller, undertakes to process personal data in accordance with the applicable legislation relating to the protection of individuals with regard to the processing of personal data and with the Privacy Statement which can be consulted on www.ing.lu or in a bank's branch on request.

Personal data communicated within the framework of subscription and use of the card and, if necessary, subsequently as part of the operations related to its use, are processed by the Bank in particular for the purpose of managing accounts and payments, granting and managing credit facilities, commercial promotion of banking services (unless the primary account-holder and cardholder, upon request and free of charge, object to direct marketing), insurance and support services, managing the relationship with the primary account-holder and the cardholder, controlling operations and preventing irregularities and fraud and managing possible litigation or recovery. These data may be communicated to other entities within ING Group engaged in banking, insurance or financial activities (list available on request) for the purposes of centralised customer management, sales promotion (unless the data subject concerned, upon request and free of charge, objects to direct marketing), managing the primary account-holder and cardholder's relationship, providing their services (if any) and monitoring the regularity of the transactions (including the prevention of irregularities and fraud). Personal data can also be communicated to insurance companies outside ING Group established in the European Union as well as the suppliers printing the cards.

The primary card account-holder and the cardholder expressly authorise the Bank and Visa to communicate to any interested and duly authorised third party their personal data required to ensure its operation within the Visa Network both in and outside the European Union and any data required to ensure the security of payments, particularly once the card has been blocked.

17. Miscellaneous

17.1. The cardholder may not use the card to make illegal purchases or obtain illegal services. Notwithstanding the foregoing, the primary card account-holder and/or the cardholder shall remain bound to pay to the Bank the totality of any amounts debited from the card account.
17.2. The primary card account-holder authorises the Bank to verify the validity of information, notably financial information, provided in relation to the card application, both while the application is being processed and throughout the term of the contract.
17.3. The Bank elects domicile at its Registered Office in Luxembourg.
17.4. The primary card account-holder elects domicile at the office of the Public Prosecutor at Luxembourg District Court, at which elected domicile any writs and other instruments will be validly served, without prejudice to the Bank's right to take exclusive account of the actual domicile of the primary card account-holder; however, the Bank will reserve the right to serve documents at the most recent address indicated by the primary card account-holder.

18. Applicable law - Competent jurisdiction

All rights and obligations of the primary card account-holder, additional cardholder and Third Party Guarantor vis-a-vis the Bank will be subject to Luxembourg law, unless expressly stipulated to the contrary. Any legal dispute, including as regards any non-contractual matters) shall be brought before Luxembourg District Courts in the absence of any express provision to the contrary.
However, the Bank reserves a discretionary right to bring any dispute before the domicile of the opposing party.

19. Application of the Bank's General Terms and Conditions and tariffs

For all other matters please refer to the Bank's General Terms and Conditions and tariffs in force which shall apply unless otherwise expressly stipulated herein.
By their signature below, the primary card account-holder and/or the cardholder and/or the Third Party Guarantor(s) declare(s) that they have received a copy of the Bank's General Terms and Conditions, these General Terms and Conditions Visa – CyberCard, and that they have understood their contents and scope, and that they expressly accept all clauses, in particular Articles 2.3., 3.2., 3.3., 5.6., 7.2., 7.4., 8, 9, 10, 12 to 18 of these Visa General Terms and Conditions Visa CyberCard.