GENERAL CARD OPERATING CONDITIONS

PRELIMINARY ARTICLE

The card (hereinafter the "Card") is issued by XPollens (hereinafter the "Issuer"), of which it remains the property, at the request of its customers, to the latter and/or their duly authorized representatives ("Cardholder"), and subject to acceptance of the request by the Issuer. The Card is issued to the Cardholder in accordance with the procedures specified by the Issuer. BD MULTIMEDIA is hereinafter referred to as the "Partner".

Where the Issuer may not issue a Card, it shall inform the Partner of the reasons for its decision.

The Card is strictly personal, and as soon as it is received, the Cardholder must sign it there is a space provided for this purpose on the Card. The absence of a signature on the Card justifies its refusal to be accepted.

To activate the Card, the Cardholder must make an initial physical purchase on an Eftpos terminal by entering the PIN code.

The Cardholder is strictly prohibited from lending or disposing of the Card.

The Issuer prohibits the Cardholder from affixing adhesive labels or stickers or from making any inscription on the Card with the exception of the signature referred to above.

The Cardholder shall refrain making any functional or physical alteration to the Card of any kind whatsoever, and in particular from interfering with its operation and that of electronic payment terminals (hereinafter "Eftpos terminals"), automatic teller machines (hereinafter collectively "Electronic Equipment") in any way whatsoever, and automatic teller machines (hereinafter "ATMs") in any way whatsoever.

The Cardholder undertakes to use the Card and its number exclusively within the framework of the payment card scheme(s) whose mark(s) is (are) affixed to the Card and to comply with the rules relating to each of the said schemes set out in the present contract.

A Payment Card scheme is a single set of rules governing the execution payment transactions linked to a Card (e.g. "Visa"). The brand name of the Payment Card scheme appears on the Card, and when the payment transaction is carried out under this brand name, the rules of the said Payment Card scheme apply to the execution of this payment transaction, under the conditions specified in the present contract and in compliance with French law applicable to the present contract.

Part 1 of this contract defines the operating rules of the Card independently of the specific rules of the payment card scheme(s) whose brand(s) appear(s) on the Card, Part 2 defines the said specific rules and Part 3 defines the functionalities to be chosen by the Cardholder.

Definitions

Unless otherwise specified, capitalized terms used in this contract the meanings given below. These terms are used indiscriminately in the singular or plural.

- **Agent** : Payment service providers may use the services one or more agents to carry out payment service activities on their behalf, within the limits of their authorization, in accordance with the provisions of article L. 523-1 of the French Monetary and Financial Code. For the purposes hereof, the Partner is XPollens' Agent.
- **Payment card or Card**: Visa payment card in the Customer's name, issued by XPollens. It is valid for three years from the date of issue.
- **Payment Account or Account**: refers to the payment account within meaning of article L. 314-1 of the French Monetary and Financial Code, opened in XPollens' books for the purpose of debiting and crediting Payment Transactions, charges due by the Account Holder and any reversals in connection with his transactions, and offsetting these amounts on the date of entry in order to show a net balance.
- **Partner's General Terms and Conditions of Use**: refers to the general terms and conditions of use agreed between the Cardholder and the Partner.
- **Contract**: refers to the present general terms and conditions of Card operation.
- **Payment Transaction**: means any payment, transfer or withdrawal of funds resulting a payment order and which may be initiated :
    - □ by the payer giving a payment order to his bank (e.g. a bank transfer);
    - □ by the payer, via the payee who, after receiving the payer's payment order, forwards it to the payer's bank, if necessary via his own bank (e.g. payment by bank card);
    - □ by the payee giving a payment order, via its own bank, to the payer's bank based on the consent given by the payer to the payee (e.g. a direct debit).

- **Partner:** means BD MULTIMEDIA, owner of the Mobile Application. The Partner is registered as an XPollens Payment Service Agent with the ACPR.
- **Mobile application**: refers to the Partner's mobile application enabling the Customer to access the payment services offered by XPollens.

- **Cardholder(s)**: means the holder(s) of the Card and of the Payment Account attached to the Card, natural person(s) of legal age not acting for the purposes of his/her professional activity (commercial, industrial, artisanal, liberal or agricultural), customer(s) of the Partner, having accepted the Partner's General Terms and Conditions of Use, as well as the present contract.

PART 1
GENERAL CARD OPERATING CONDITIONS COMMON TO ALL PAYMENT CARD SCHEMES

ARTICLE 1: PURPOSE OF THE CARD

1.1 The Card is a payment instrument for the exclusive use of the systematically authorized Cardholder, enabling him/her to carry out payment transactions, for the sole purpose of :

- withdraw cash in France or abroad:
  - at ATMs displaying the brand(s) affixed to the Card,
  - at the counters of establishments duly authorized provide payment services displaying the same brand(s) and equipped with Eftpos terminals, within the limits of the paying counter's availability and upon presentation of a valid form of identification;
- pay for goods or services purchased from acceptors equipped with Electronic Equipment or a remote acceptance system, and displaying the mark(s) affixed to the Card. However, the systematic authorization Card is not accepted from acceptors equipped with Electronic Equipment that does not have the technical capability to issue an authorization request.
- pay donations or subscriptions to any entity duly authorized to collect or receive them, and displaying brand(s) affixed to the Card;
- transfer funds to any person who is either duly authorized to receive such funds and displays the mark(s) affixed to the Card, or who is the holder of a Card bearing the same mark or a mark enabling funds to be transferred by Card, through a duly authorized payment service provider displaying the mark(s) affixed to the Card.

1.3 Where applicable, the Card described above also enables access to other services offered by the Issuer and governed by specific provisions.

1.4 This Card is for non-business use only. The Cardholder agrees not to use the Card for purpose other than those described above.

1.5 The Card is systematically authorized and debited immediately.

Pursuant to EU Regulation 2015/751 of April 29, 2015, Cards issued in the European Economic Area (the Member States of the European Union, Iceland, Liechtenstein and Norway - hereinafter the "EEA"), and the DROM territories are classified in one of the following four categories:

- flow,
- credit,
- prepaid,
- commercial.

The "debit" category includes immediate debit Cards. These cards are marked "Debit".

The "credit" category includes deferred debit cards and/or cards backed by revolving credit, as defined by the French Consumer Code. They are labelled either "Credit" for deferred debit cards, or Credit Card" for cards backed a revolving credit as defined by the French Consumer Code.

The "prepaid" category refers to cards used to store electronic money. They are marked "Prepaid".

The "Commercial" category includes Cards intended payment of business expenses and whose payment transactions are debited directly from a business account. They are marked "Commercial" and are not governed by these terms and conditions.

The Acceptor may decide not to accept all Card categories.

In this case, the Acceptor must inform the Cardholder clearly and unambiguously. Before making a payment, the Cardholder must check that the category of Card he/she holds is accepted by the Acceptor.

ARTICLE 2: PERSONAL SECURITY DATA AND STRONG AUTHENTICATION

Personalized security data is personalized data provided to the Cardholder by the Issuer for authentication purposes.

The Issuer implements a strong Cardholder authentication system for Card payment transactions initiated by the Cardholder in accordance with the terms and conditions set out in Delegated Regulation EU 2018/389 of November 27, 2017, when the application of this strong authentication is required by the said Regulation.

The Card Issuer may apply exceptions to the implementation of strong authentication devices for the Cardholder under the conditions and in accordance with the limitations set out in Delegated Regulation EU 2018/389 of November 27, 2017.

A strong authentication system implemented by the Issuer is based on the use of at least two elements belonging to the categories "knowledge" (something that only the Cardholder knows), "possession" (something that only the Cardholder possesses) and "inherence" (something that the Cardholder is).

2.1 Sending the Card and Confidential Code (hereinafter "Code")

The Payment Card is automatically ordered and sent to the postal address indicated by the Customer in the Mobile Application, or collected from a point of sale (Visa Classic only).

The Issuer sends the Cardholder a Code for the use of his Physical Card in his mobile Application.

The number of successive attempts to enter the Code is limited to 3 (three) on Electronic Equipment and ATMs. On the third unsuccessful attempt, the Cardholder will cause the Card to be invalidated and/or captured.

2.2 Other customized safety data

The Issuer may provide the Cardholder with other personalized security data:

- to make remote payment transactions with his Physical Card on websites displaying the "CB" or "Verified by Visa" or "MasterCard SecureCode" logo:
    - o By using the strong authentication offered by the Issuer, enabling the to authenticate himself on his smartphone using his validation code or the smartphone's biometric function. The Cardholder must have previously activated this authentication solution on the Mobile Application, be a Cardholder, and have a compatible smartphone whose telephone number has been previously communicated to the Issuer and which is associated this solution. During the payment transaction on the website, the Cardholder enters his or her Card number, expiry date and the three-digit visual cryptogram on the back of the Card, and validates his or her entry. This generates the opening of the authentication solution on the Cardholder's smartphone. The Cardholder is asked to confirm the operation, either by entering the validation code he/she defined when activating the solution, or by using the biometric function on his/her smartphone.
        - o Or by communicating a single-use code (hereinafter referred to as the "Authentication Code") by text message sent to the Cardholder on the cell phone number previously communicated to the Issuer. During the payment transaction on the website, the Cardholder enters his Physical Card number, expiry date and the three-digit visual cryptogram on the back of his Physical Card, and validates his entry. This immediately generates the sending of a Cardholder Authentication Code by SMS. The Cardholder must then enter the Authentication Code on the payment page displaying the Issuer's logo, and validate his or her entry.

2.3 Cardholder security obligations

The Cardholder must use the personalized security data and the strong authentication devices set up by the Issuer whenever instructed to do so by the Card acceptance devices, failing which he/she will be held liable.

The Cardholder must take all appropriate measures to ensure the security of the Card, the Code and, more generally, all personalized security data (in particular the Authentication Code). He must therefore keep his Code and the Authentication Code transmitted during an Internet payment absolutely secret, and not communicate them to anyone. In particular, he must not write his Code on the Card, or on any other document. He/she must ensure that he/she composes it away from prying eyes.

In addition, where a strong authentication device set up by the Issuer is used, the Cardholder must take all necessary measures to prevent (i) the disclosure to unauthorized third parties of authentication factors belonging to the "knowledge" category, and/or (ii) the copying of authentication factors belonging the "possession" category, and/or (iii) any unauthorized use of factors belonging to the "inherence" category.

ARTICLE 3: FORM OF CONSENT AND IRREVOCABILITY

When a payment transaction is made to an Acceptor, the Electronic Equipment and/or the remote acceptance system - subject to the availability of the necessary technology - offers the Cardholder the choice of the payment Card scheme, the brand of which appears on the Card, that he/she wishes to use to carry out the payment transaction.

The Acceptor may propose the selection of a Payment Card scheme that the Cardholder is free to modify.

3.1 The Cardholder and the Issuer (hereinafter the "Parties") agree that the Cardholder gives his consent to carry out a payment transaction before or after the amount has been determined:

- by entering the Code on the keypad of an ATM or Electronic Equipment, checking for the presence of the mark(s) on the Card;

- by inserting the Card into Electronic Equipment without a keypad for entering the code and displaying the mark(s) on the Card;

- remotely, by communicating to the Acceptor displaying the mark(s) affixed to the Card and/or confirming the data related to remote use of its

Card, in particular, when required, by compliance with any strong authentication system set up by the Issuer;

- by confirming the payment order data communicated via a digital wallet to the Acceptor displaying the mark(s) affixed to the Card;

- by presenting and holding the Card in front of a device that identifies the presence of contactless technology. This kinematics is also valid when the Card is dematerialized and integrated into another medium, such as a cell phone for example;

- compliance with any strong authentication set up by the Issuer to validate use of the Card.

3.2 Recurring payments

The Cardholder may use the Card for a series of payment transactions (hereinafter referred to as "recurring payments") for purchases of goods and/or services.

The Cardholder consents to the following series of transactions:

- remotely, by communicating and/or confirming the data relating to the remote use of the Card at the time of the first transaction,
- and, if applicable, via a digital wallet, at the time of the first transaction.

The first payment transaction then complies with article 3.1.

Subsequent transactions initiated by the Acceptor are not subject to strong authentication.

3.3 Pre-authorization linked to payment a service

The Cardholder may give his or her consent to the execution of a payment transaction prior to the start of service (e.ghotel room rental, car rental, purchase of fuel from an ATM, and, in certain cases, payment a transport service at a kiosk) for a maximum amount known and agreed with the Acceptor. The final amount of the payment transaction is determined at the end of the service.

The maximum amount thus authorized may have an impact on the payment limits set and notified by the Issuer.

3.4 Irrevocability of payment orders

The payment transaction is authorized if the Cardholder has given his consent in one of the forms defined above.

From that moment on, the payment order is irrevocable.

However, the Cardholder may stop payment in the event of the Acceptor's receivership or liquidation proceedings, as long as the account of the Acceptor's payment service provider has not been credited with the amount of the payment transaction.

In addition, for recurring and/or staggered payments, the Cardholder may withdraw his consent to the execution of a payment transaction or series of payment transactions for the future, no later than the end of the working day preceding the day agreed for its execution.

The Issuer is not involved in any dispute other than that relating to the payment order, which may arise between the Cardholder and the Acceptor. Under no circumstances may the existence of such a dispute justify a refusal by the Cardholder and/or the payment account to which the Card is attached to honour the payment.

ARTICLE 4: TERMS OF USE OF THE CARD FOR CASH WITHDRAWALS IN FRANCE AND ABROAD AT DAB/GAB ATMS

4.1 Cash withdrawals in France or abroad are possible within the limits set and notified by the Issuer in this contract or in any document approved by the Issuer.

the Cardholder and/or the deposit account to which the Card is attached.

4.2 The Cardholder and/or the deposit account to which the Card is attached must, prior to each withdrawal and under his own responsibility, ensure the existence of a sufficient and available balance in the said account, and maintain it until the corresponding debit is made.

4.3 The amounts recorded for these withdrawals, as well as any commissions, are debited from the deposit account to which the Card is attached, within the usual time limits for cash withdrawals in France or abroad. The amount of these transactions is shown on the transaction statement referred to in article 5.6. The Cardholder is informed that certain establishments duly authorized to provide payment services charge the access fees (or "ATM Fees") at their ATMs displaying the mark(s) affixed to the Card, for cash withdrawals in France or abroad. These establishments must inform the by any appropriate means prior to the withdrawal.

ARTICLE 5: TERMS AND CONDITIONS FOR USING THE CARD TO PAY FOR GOODS AND SERVICES PURCHASED FROM ACCEPTORS

5.1 The Card is a payment instrument that may only be used to pay for goods and services purchased from acceptors who are members of the payment card scheme(s) whose brand(s) is (are) affixed to the Card.

5.2 These payment transactions are possible within the limits set and notified by the Issuer in this contract or in any document approved by the and/or the Payment Account to which the Card is attached.

5.3 Card payments are made in accordance with the conditions and procedures in force at acceptors who have adhered to one of the payment card schemes whose mark(s) is (are) affixed to the Card. In principle, these conditions and procedures include a check of personalized security data and, under certain conditions defined by the payment card schemes, a request for authorization.

The Acceptor may install a priority selection mechanism for a brand or payment application on the Electronic Equipment. The Cardholder may override the automatic priority selection proposed by the Acceptor in his Electronic Equipment by choosing another brand affixed to his Card or another payment application, insofar as it displayed as "accepted" by the Acceptor.

The Cardholder may store data linked to his or her Card in digital merchant environments (e-commerce sites, mobile applications, etc.), particularly for recurring and/or staggered payments. This Card data may be stored in the form of tokens linked to specific devices and/or areas of use, which are used for payment purposes (the
"Token(s)"). Each Token has a unique number, and can be activated or deactivated independently of the Card. If the Acceptor stores the Card data in the form of a Token given by the Issuer, this Token may be updated automatically by the Issuer when the Physical Card is renewed. Card payments may therefore continue to be made with this Acceptor, the Cardholder having to

enter his new Physical Card data instead of the Physical Card data he had originally registered.

The Issuer may also make available to the Cardholder an option enabling him to activate or deactivate the remote payment function of his Card described in Part 3 of these General Terms and Conditions.

5.4 Payment transactions received by the Issuer are automatically debited to the Payment Account to which the Card is attached in accordance with the provisions agreed between the Cardholder and the Issuer in this contract or in any document approved by the Cardholder and/or the Payment Account to which the Card is attached.

Even if these agreements provide for deferred payment, the Issuer may immediately debit the account for the amount of payment transactions carried out using the Card in the event of death, legal incapacity of the Cardholder and/or the holder of the Payment Account to which the Card is attached, payment incidents (payment transactions not covered by the account balance or by an overdraft authorization, bank or legal prohibition) or of the operation of the account (any seizure or administrative seizure by a third party, blocking in the event of denunciation of a joint or undivided account), closure of the account or withdrawal of the Card by the Issuer, a decision which will be notified to the Cardholder and/or the holder of the Payment Account to which the Card is attached by simple letter.

Likewise, the Issuer is entitled to immediately debit the Payment Account to which the Card is attached with the amount of the payment transactions carried out using the Card if the total number of payment transactions exceeds the limits set and notified by the Issuer.

For payment orders given online, the Cardholder may be required to comply with a procedure for security purposes as described in article 2.2 above.

5.5 As the Card is an immediate debit card, the Cardholder and/or the Payment Account to which the Card is attached must, prior to each payment transaction and under his/her own responsibility, ensure that there is a sufficient and available balance on the Payment Account to which the Card is attached, and maintain it until the corresponding debit is made.

5.6 The detailed amount (amount, commissions, exchange rate) of Card payment transactions debited to the payment account to which the Card is attached appears on a transaction statement that can be consulted and downloaded from the Mobile Application.

5.7 It can also be consulted electronically on the Mobile Application. It is the responsibility of the holder of the Payment Account to which the Card is attached to verify without delay the regularity of payment transactions appearing on the transaction statement as soon as it is received or made available on the Mobile Application.

ARTICLE 6: TERMS AND CONDITIONS FOR USING THE CONTACTLESS CARD TO PAY FOR GOODS AND SERVICES PURCHASED FROM ACCEPTORS

6.1 Contactless" technology enables the rapid payment of goods or services using the electronic equipment of acceptors equipped for this purpose, with remote reading of the card without the need to enter a code.

Unless otherwise instructed by the Cardholder when subscribing to the present contract or prior to renewal of the Card, the Issuer provides the Cardholder with a Card that can be used in "contactless" mode.

6.2 In all circumstances, the Cardholder must comply with the instructions displayed on the Electronic Equipment located at the Acceptor's premises.

6.3 In the event of payment in "contactless" mode with use of the Physical Card, the Issuer does not apply the Cardholder's strong authentication devices that it has put in place, under the conditions and in accordance with the procedures set out in Delegated Regulation EU 2018/389 of November 27, 2017.

These rules define the maximum unit amount of each payment transaction in contactless mode, and the maximum cumulative amount of successive payments in contactless mode, or the maximum number payment transactions in contactless mode. For security purposes, these ceilings may be limited by the specific rules of payment card scheme used for the payment transaction. These limits are specified in Part 2 of the present contract.

Beyond this number of successive authorized transactions or this accumulated amount, the must carry out a payment transaction by entering the Code, in order to continue using the Card in "contactless" mode, and to reset the accumulated amount or the maximum accumulated number available.

6.4 In the event of use of a machine offering only the possibility of accepting payment in "contactless" mode, the Cardholder is hereby informed and accepts that his payment may be refused in accordance with the provisions of the present article, and that in this case it may be necessary to :

- a payment in conventional contact mode with code entry elsewhere than on said vending machine where
- a withdrawal before being able to use the aforementioned payment machine.

6.5 Payment transactions in "contactless" mode received by the Issuer are automatically debited to the Payment Account to which the Card is attached on the basis of the records of these payment transactions in the acceptance systems or their reproduction on a durable computer medium.

The payment transaction may be recorded on the ticket issued by the Electronic Equipment located at the Acceptor's premises.

ARTICLE 7: RECEIPT AND EXECUTION OF PAYMENT

The Issuer informs the Cardholder that the payment order has been received by the Issuer at the time it is communicated to the Issuer by the Acceptor's payment service provider through the clearing or settlement system for the said payment order.

When the payment order is executed within European Economic Area and the French overseas territories, the Issuer has a period of one business day from the time of receipt to credit the account of the Acceptor's payment service provider.

ARTICLE 8: ISSUER'S LIABILITY

8.1 Where the Cardholder denies having given his consent to carry out a payment transaction, it is the responsibility of the Issuer to provide proof that the transaction has been authenticated, duly recorded and accounted for in accordance with the state of the art, and that it has not been affected by a technical deficiency. This proof may be provided by any means, in particular by Electronic Equipment recordings or their reproduction on a computer medium of the use of the Card and personalized security data.

The Issuer may use these records to justify their allocation to the Payment Account to which the Card is attached.

8.2 The Issuer is liable for direct losses incurred by the Cardholder due to a technical deficiency in the Payment Card scheme over which the Issuer has direct control.

However, the Issuer shall not be held liable for any loss due to a technical defect in the payment card scheme, if such defect is indicated to the Cardholder by a message on Electronic Equipment or some other visible way.

ARTICLE 9: OPPOSITION OR BLOCKING REQUESTS

For the purposes of this contract, the above-mentioned "blocking" information may also be referred to as "opposition".

9.1 As soon as he becomes aware of the loss or theft of the Card, its misappropriation or any fraudulent use of the Card or of the data linked to its use, the Holder of the Card and/or of the Payment Account to which the Card is linked must inform the Issuer without delay in order to block his Card, indicating the reasons for which he is requesting the blocking.

9.2 This opposition (or blocking) request must be made :

- to the Issuer during its opening hours, in particular by telephone, on the Mobile Application by activating the functionality described in Part 3 of these General Terms and Conditions;
- or, in general, to the Opposition Center, open 7 days a week, hours a day, by calling 09 69 32 00 61.

9.3 The blocking request is processed immediately. The Issuer may not be held liable for the consequences of a blocking request made by telephone, Internet or .... that does not originate from the Cardholder and/or the Payment Account to which the Card is attached.

A registration number for this blocking request is communicated to the Cardholder and/or the payment account to which the Card is attached, which it is the Cardholder's responsibility note down. From the date of this blocking request, the Issuer will keep the information relating to the request for a period of eighteen (18) months, and will provide this information upon request by the Cardholder and/or the payment account to which the Card is linked during the same period.

9.4 The circumstances of the loss or theft of the Card, its misappropriation, or any fraudulent use of the Card, must be investigated.

Any loss or damage to the Card or to data relating to its use must be declared in writing and signed by the Card and/or Account Holder, by letter delivered or sent by registered post, to the counter holding the Payment Account to which the Card is attached.

In the event of theft or fraudulent use of the Card or misappropriation of the data linked to its use, the Issuer may request a receipt or a copy of a complaint or the receipt of the online report, on the Percev@l platform of the French Ministry of the Interior, of fraudulent use of the Card during an online purchase.

This request is not a condition for reimbursement of the disputed transactions.

The Cardholder authorizes the Issuer to use the information provided by the Cardholder in connection with the opposition request, in particular to enable the Issuer to file a complaint.

ARTICLE 10: LIABILITY OF THE CARDHOLDER AND THE ISSUER

10.1 Principle

The Cardholder must take all measures to preserve his Card and the personalized security data attached to it, in particular his Code or any strong authentication element belonging to the "knowledge", "possession" and "inherence" categories. It must be used for the purposes specified in article 1.

As indicated in article 11.2, he/she assumes the consequences of using the Card until such time as he/she has requested opposition (or blocking) under the conditions set out in article 9.

10.2 Unauthorized transactions carried out prior to the opposition (or blocking) request

Transactions resulting from loss or theft of the Card will be charged to the Cardholder up to a maximum of 50 euros; however, the Cardholder will not be held liable:

- in the event of a payment transaction carried out without the use of personalized security data ;
- if the loss or theft of the Card could not be detected by the Cardholder prior to payment;
- when the loss of the Card is due to acts or omissions of an employee, agent or branch of the Issuer or of an entity to which the Issuer has outsourced its activities.

However, if the Acceptor's payment service provider is located outside European Economic Area, French overseas departments and territories, Saint Pierre et Miquelon or Saint Barthélemy, the Cardholder will be liable for up to 50 euros for transactions resulting from the loss or theft of the Card, even in the case of payment transactions carried out without the use of personalized security data.

The Issuer is liable for any unauthorized transactions resulting from counterfeiting of the Card or unauthorized use of data related to the use of the Card.

10.3 Unauthorized transactions carried out after the opposition (or blocking) request has been made

The Issuer is also responsible for any such costs, with exception of those incurred by the Cardholder.

10.4 Exceptions

All unauthorized transactions are the responsibility of the Cardholder, with no limit on the amount in the event of :

- intentional or grossly negligent breach of the obligations referred to in the Preliminary Article and in articles 2, 5.7, 7.7, 9.1 and 9.2 ;
- fraudulent acts by the Cardholder.

Unless the Cardholder has acted fraudulently, the Cardholder shall bear no financial consequences if the unauthorized Payment Transaction was carried out without the Issuer requiring strong authentication of the Cardholder in compliance with the strong authentication procedure implemented by the Issuer.

ARTICLE 11: CONTRACT DURATION AND TERMINATION

11.1 The present contract is concluded for a fixed period of three years (corresponding to the period of validity of the Card). It comes into force on the date of acceptance by the Cardholder. It will be automatically renewed each time a new Card is received, for successive periods of three years, unless terminated in accordance with article 11.2 below.

11.2 It may be terminated at any time in writing with acknowledgement of receipt by the Cardholder or the payment account to which the Card is attached, or by the Issuer. Termination by the Cardholder takes effect thirty (30) days after the date on which notice is sent to the Issuer. Termination by the Issuer takes effect two (2) months after the date on which notice is sent to the Cardholder, except in the case referred to in Article 12.

11.3 The holder of the Card and/or the payment account to which the Card is attached undertakes to return the Card and to comply with all the contractual obligations incumbent upon him/her under the present contract, until such time as the above-mentioned termination takes effect.

11.4 As of the effective date of termination, the Cardholder is no longer entitled to use the Card and the Issuer may take any measures necessary to do so.

ARTICLE 12: CARD VALIDITY - RENEWAL, BLOCKING AND RETURN OF THE CARD

12.1 The Card has a validity period, the expiry date of which is indicated on the Card itself. Card is valid for thirty-six months.

12.2. At its expiry date, the Card is renewed every thirty-six months. In order proceed with this renewal, the Cardholder must order
its new Card via its mobile Application.

12.3 The Issuer may contact the Cardholder by any appropriate means in the event of suspected or proven fraud or a threat to security.

12.4 In addition to cases of blocking resulting from account management, the Issuer may block the Card for reasons security or presumption of unauthorized or fraudulent transactions, or in the event of a significantly increased or proven risk that the Cardholder and/or the Payment Account to which the Card is attached may be unable to meet his payment obligation.

12.5 In all cases, the Cardholder and/or the Payment Account to which the Card is attached will be notified of the reason for the blocking decision by any means available.

12.6 The Cardholder therefore undertakes to return the Card on first request, and agrees not to make any use of it.

12.7 Closure of the Payment Account to which a Card is attached entails the obligation to return the Card(s). The earliest that the account can be definitively closed is one (1) month after the return of the Card(s).

12.8 When the Cardholder registers his Card data with an Acceptor, and the Acceptor stores this data in form of a Token, in accordance with article 5.3 of Part 1 of this contract, this Token may be updated automatically on the expiry date of the Physical Card. The Cardholder will then be able to continue to make payments by Card at the said Acceptor, without having to enter the data of the renewed Physical Card, instead of the data of the expired Physical Card that the Cardholder had initially registered.

ARTICLE 13: DISPUTES

13.1 The Cardholder of the Card and/or of the Payment Account to which the Card is attached may dispute a transaction with the Issuer, if possible by presenting the ticket issued by the Eftpos terminal or proof of the payment order to which the dispute relates, **as quickly as possible** and within a maximum period of thirteen (13) months from the date of the disputed payment transaction charged to the Payment Account to which the Card is attached.

The maximum period during which the Cardholder and/or the Payment Account to which the Card is attached may dispute a Transaction seventy (70) days from the date of the disputed Payment charged to the said account, when the Acceptor's payment service provider is located outside the European Economic Area, the French overseas departments and territories of Saint Pierre et Miquelon or Saint Barthélemy.

For disputes concerning funds transfers credited to the account, the ticket issued by the electronic equipment or remote system of merchant or service provider who ordered the funds transfer is not proof of the funds transfer transaction.

13.2 The Cardholder is entitled to reimbursement of an authorized Payment Transaction carried out within the European Economic Area and French overseas departments and territories, if the authorization given did not indicate the exact amount of the transaction and if the amount of the Payment Transaction exceeds the amount that the Cardholder may reasonably expect. In this case, the Issuer may ask the Cardholder to provide all information relating to the requested reimbursement.

The request for reimbursement must be made within eight (8) weeks of date on which the payment order for which reimbursement is requested was debited from the Payment Account to which the Card is attached.

The Issuer has a period of ten (10) business days from receipt of the request for redemption to make the redemption or to justify its refusal make the redemption.

13.3 The parties agree to take the utmost care informing each other of the terms and conditions of the transaction.

ARTICLE 14: REIMBURSEMENT FOR UNAUTHORIZED OR INCORRECTLY EXECUTED TRANSACTIONS

14.1 Unauthorized payment transaction

The Cardholder and/or the Payment Account to which the Card is attached will be reimbursed immediately and at the latest on the first working day following receipt of the transaction dispute:

- the amount of the transaction disputed in good faith by the Cardholder in the event of loss and/or theft, fraudulent use and/or misappropriation of the Card and related data, which occurred prior to the request to stop (or block) the transaction under the conditions set out in article 10.2 ;
- of the amount of the transaction contested in good faith by the Cardholder, occurring after the request for opposition (or blocking) in accordance with article 10.3.

The Issuer may nevertheless reverse the amount of the reimbursement thus made, by informing the Cardholder and/or the Payment Account to which the Card is attached, in the event that it is able either to establish that the transaction in question was indeed authorized or to provide evidence of fraud or gross negligence committed by the Cardholder.

However, in accordance with legal provisions, the Issuer will not proceed with reimbursement within the aforementioned period if it has good reason to suspect fraud on the part of the Cardholder. In this case, the Issuer will inform the Banque de France.

14.2 Poorly executed payment transaction

The Cardholder and/or the Payment Account to which the Card is attached is reimbursed, if necessary and without delay, for the amount of the incorrectly executed transaction.

14.3 Common provisions

In all the cases listed above, the debited account is restored the state it would have been in had the disputed amounts not been debited, and to the correct value date.

ARTICLE 15: PROTECTION OF PERSONAL DATA

15.1 In connection with the signing and performance of this contract, the Issuer, acting as data controller, collects and processes personal data concerning the Cardholder and/or the Payment Account to which the Card is attached.

The categories of personal data processed are :

- information collected under this contract,
- those shown on the Card and those generated from it,
- and those relating to transactions carried out using the Card.

This information will be processed, automatically or otherwise, for the following purposes, i.e. to enable :

- manufacturing the Card, managing its operation and ensuring the security of payment transactions, in particular when the Card is blocked. This processing is necessary for the proper execution of the present contract, failing which the contract cannot be executed;
- automatic updating of Card data, in the event of renewal, when the Card is registered in digital merchant environments (e-commerce sites, mobile applications, etc.), in particular for recurring and/or staggered payments, by virtue of the Issuer's legitimate interest;
- automatic updating of Tokens linked to the Card, in the event of renewal of the Card, by virtue of the Issuer's legitimate interest;
- to prevent and combat card payment fraud, by virtue of the Issuer's legitimate interest;
- the management of any legal action taken by virtue of the Issuer's legitimate interest;
- to meet the Issuer's regulatory or legal obligations, particularly in criminal or administrative matters relating to the use of the Card.

In order to authenticate the Cardholder and/or prior to authorizing a payment transaction, the Issuer may implement automated decision-making based in particular on the analysis of the Cardholder's personal data, the context of the transaction, the balance of the Payment Account to which the Card is attached and the Card's usage limits.

Necessary for the proper execution of the contract, automated decision-making may lead to the authorization or refusal of the Payment Transaction.

15.2 The Cardholder has the right express his or her point of view and to contest the automatic decision referred to in article
15.1 by contacting :

Data Protection Officer for Pôle Payments entities

BP 4 - 75060 Paris Cedex 02 France 9

E-mail dpo-xpollens@bpce.fr

15.3 Further information on how long the personal data processed is kept, to whom it may or must be communicated by the Issuer, and what rights the and/or the payment account to which the Card is attached has in respect of his or her data can be found in the Issuer's Information Notice, available on the Mobile Application.

ARTICLE 16: FINANCIAL CONDITIONS

In return for the payment services provided, the Account Holder shall pay the Partner the fees agreed in the Partner's General Terms and Conditions.

In addition, under the present terms and conditions, for the maintenance of an inactive Account, the fees and commissions due annually on inactive Accounts are €30 including tax, which will be deducted from the credit balance of the Account.

The Licensee expressly authorizes XPollens to pay any fees due and payable under the Contract or the Terms and Conditions.

General Terms and Conditions by deduction from the Partner's Account, within the limit of the available balance.

The Parties agree that the reciprocal debts of XPollens and the Account Holder resulting from the execution of the Agreement or the Partner's General Terms and Conditions, are automatically transformed into simple credit and debit items within the limit of the available provision of the Account. After offsetting, these debits and credits form a net credit or zero balance on the Account. In the absence of sufficient funds on the Account, the amount remaining due by the Account Holder after offsetting is shown on the Account statement on a specific line corresponding to a debt due.

ARTICLE 17: PENALTIES

Any false declaration is punishable by law.

Any misrepresentation or misuse of the Card may also result in termination as provided for article 11 of the present contract.

Any actual costs and expenses incurred in enforcing recovery of transactions under an enforceable title shall be borne jointly and severally by the Cardholder and/or the Payment Account to which the Card is attached.

ARTICLE 18: CHANGES TO CONTRACT CONDITIONS

The Issuer reserves the right to make changes, in particular financial changes, to the present contract, which will be communicated on paper or on any other durable medium to the Cardholder and/or the Payment Account to which the Card is attached, two (2) months prior to the date their entry into force. Failure to notify the Issuer of any objection before the expiry of the aforementioned period shall constitute acceptance of such modifications. In the event that the Cardholder and/or the Payment Account to which the Card is attached do not accept the modifications, they have the right to terminate the present contract immediately and without charge before the date on which the modifications come into force.

Any legislative or regulatory provisions that make it necessary to modify all or part of the present contract are applicable from their date of entry into force.

ARTICLE 19: COMPLAINTS - MEDIATION

In the event of difficulties concerning these products and services, the Cardholder and/or the holder of the payment account to which the Card is attached may obtain the information required from the Partner, submit any complaint to the Partner and, in the event of persistent difficulties, contact the Partner in writing at the following e-mail address:

contact@toneofirst.fr or by phone at 0153362424

The Partner undertakes to reply to the Licensee within ten (10) working days. However, if a more in-depth analysis of the file is necessary and results in the deadline being exceeded, the Partner undertakes to inform the Licensee of the new deadline which, except in very special cases, should not exceed two (2) months (from the date of receipt of the claim).

In the case of complaints relating to payment services, the Cardholder and/or the Payment Account to which the Card is linked will receive a reply within fifteen (15) working days of receipt of the complaint. However, if additional time is required to respond, XPollens or the Partner will send a response explaining the delay and specifying the final date of the response. In any event, the Cardholder and/or the payment account to which the Card is linked will receive a definitive response no later than thirty-five (35) working days following receipt of the complaint.
In the absence of a satisfactory solution or in the absence of a response within these time limits, the Cardholder, if he/she is a consumer within the meaning of the French Consumer Code, may refer the matter free of charge to the XPollens mediator, within a period of one year from the date of the prior complaint made to XPollens:

• Or by post: Maître Carol SABA Médiateur de la consommation de l'AFEPAME, 36 rue Taitbout, 75009 Paris.

• Or submit your request for mediation directly online on the Consumer Ombudsman's website at AFEPAME https://mediateur-consommation-afepame.fr.

In the case of online subscriptions, the Cardholder and/or the holder of the payment account to which the Card is linked may also file a claim with the European online alternative dispute resolution platform, which will direct the claim: http://ec.europa.eu/consumers/odr/.

ARTICLE 20: APPLICABLE LAW AND LANGUAGE

Pre-contractual relations and this contract are governed by French law.

The language used is French for pre-contractual relations and the drafting of this contract.

PAYMENT SERVICE PROVIDER SUPERVISORY AUTHORITY :

Autorité de Contrôle Prudentiel et de Résolution, 4 Place de Budapest CS 92459, 75436 PARIS CEDEX 09.

PART 2

SPECIFIC CARD OPERATING RULES FOR PAYMENT CARD SCHEMES

The Specific Card Operating Rules (hereinafter referred to as the "Specific Rules") specific to each payment card scheme whose brand(s) is/are affixed to the Card are set out below.

The Specific Rules of the payment Card scheme chosen by the Cardholder at the time of payment apply to the Card payment transaction. Where applicable, a Payment Card scheme may establish Specific Rules for any of its Card brands.

The Specific Rules are in addition to the General Terms and Conditions of Card Operation stipulated in Part 1 of the present contract, it being specified in the event of contradiction between the latter, the Specific Rules shall take precedence over the General Terms and Conditions of Card Operation.

VISA PAYMENT CARD SCHEME ARTICLE 1 -

DEFINITION

The VISA payment card scheme determines the rules, practices, standards and/or guidelines, governing the execution of VISA-branded payment transactions with a VISA-branded Card (hereinafter the "VISA Card"), with acceptors adhering to the VISA payment card scheme (hereinafter the "VISA Acceptor") within the sole framework of the provisions and procedures defined or approved by the VISA card scheme.

The Specific Rules for the VISA Payment Card Scheme, summarized below, apply to Card payment transactions carried out by the Cardholder under the VISA brand. They are in addition to the General Card Operating Conditions set out in Part 1 of this contract.

If the Cardholder's consent is required for the purchase of a compatible VISA Card, the Cardholders legal representative or the holder of the payment account to which the VISA Card is linked acknowledges that he/she has read and accepted these terms and conditions of use and authorizes the Cardholder to activate the service.

ARTICLE 2 - FORM OF CONSENT

In addition to the terms and conditions set out in article 3 of Part 1 of this contract determining the conditions under which the Cardholder gives his consent to the Payment , the Cardholder and the Issuer agree that the Cardholder gives his consent to carry out a Payment Transaction under the VISA brand before or after the amount has been determined:

- by hand-signing the tickets issued by the Electronic Equipment to both the VISA Acceptor and the Cardholder;

- when the Card is integrated in dematerialized form into payment solutions approved by the Issuer:

  - o by presenting and holding the cell phone or any other compatible device with payment solution and "contactless" technology device /Electronic equipment identifying the presence of contactless technology and displaying the VISA trademark. Where applicable, the Cardholder may also be asked to confirm the payment order by activating the biometric function of his/her cell phone or any other device equipped with the payment solution, or, if this function is unavailable, by entering the Secret Code associated with the payment solution concerned;
  - o by confirmation of the payment order communicated via the payment solution. Where applicable, the Cardholder confirms the payment order in accordance with the procedure described in the previous paragraph.

ARTICLE 3 - PAYMENT TRANSACTIONS "CONTACTLESS'' WITH THE PHYSICAL CARD

For security purposes, the maximum unit amount of each payment transaction in "contactless" mode carried out in the VISA payment card scheme in France with the Physical Card is limited to fifty (50) euros. In addition, the Issuer may limit the cumulative amount of successive "contactless" payments to a maximum of one hundred and fifty (150) euros.)

Consequently, beyond the accumulated amount, the Cardholder must carry out a payment transaction by entering the Code in order to continue using the Card in "contactless" mode and reset the accumulated amount.

Abroad (outside France), the maximum unit amount of each payment transaction in contactless mode may vary. In addition, the Issuer may limit the maximum number and cumulative amount of successive contactless payments.

PART 3
FEATURES AT CARDHOLDER'S DISCRETION

Subject to availability, the Issuer provides the Cardholder with various Card management functions on the Mobile Application, which the Cardholder is free to use.

ARTICLE 1 - COMMON PROVISIONS

The Cardholder is responsible for activating or deactivating any of these functions. It may be subject to a strong authentication system set up by the Issuer for the Cardholder.

In principle, this activation or deactivation is operational in real time, subject to technical delays or temporary unavailability of the service (e.g. maintenance).

If the functionality is subject to a fee, this fee is specified in the Partner's General Terms and Conditions applicable to the Cardholder.

ARTICLE 2 - REMOTE PAYMENTS

This feature enables the Cardholder to activate or deactivate the "remote payment" function.

In most cases, when the option is deactivated, the Cardholder can no longer initiate remote payments, particularly over the Internet, by telephone or by post.

ARTICLE 3 - FOREIGN PAYMENTS

This feature enables the Cardholder to activate or deactivate the "foreign payments and withdrawals" function (excluding France and French overseas territories). When the option is deactivated, the Cardholder can no longer make payments requiring a request for authorization, or withdraw cash abroad. However, payments not requiring authorization will not be blocked.

ARTICLE 4 - TEMPORARY LOCKOUT

This feature allows the Cardholder to activate or deactivate the "temporary lock" function. When the option is activated, most payments in France and abroad are blocked. This blocking of the card should only be used as a temporary and preventive measure, and in no way constitutes a request to the Issuer to block the card. In the of loss, theft, misappropriation or any fraudulent use of the Card or of the data linked to its use, the Cardholder and/or the Payment Account to which the Card is linked must immediately submit a stop payment request to the Issuer in accordance with the conditions set out in these General Terms and Conditions.

ARTICLE 5 - MANAGING CEILINGS AND INCREASING THEM TEMPORARILY

The "Available Payments" and "Available Withdrawals" functionalities display the amount remaining to be used by the Cardholder in relation to the Card's payment and withdrawal limits applicable over a given period.

The "available balance" in payment is calculated by deducting from the ceiling, local payments which are subject to a request for authorization, local payments abroad (outside France) and remote payments. Deposits requested from the Card for rental purposes (e.g. car rentals) are also taken into account.

The "available balance" for withdrawals is calculated by deducting withdrawals from ATMs in France and abroad from the limit.

The amounts remaining to be used by the Cardholder in relation to these payment limits apply subject to the funds available on the payment account to which the Card is attached.

ARTICLE 6 - OPPOSITION

As soon he becomes aware of the loss or theft of his Card, its misappropriation or any fraudulent use of his Card or of the data linked to its use, the Cardholder and/or the payment account to which the Card is linked must request the Issuer to block his Card, in accordance with article 9 of these General Terms and Conditions.

This feature allows the Cardholder to request stop payment online, with immediate effect. By choosing online cancellation, the Cardholder can immediately order a new Card. The Cardholder can choose his or her own Code, or have one automatically assigned, from the mobile Application. The new Card will be delivered within five (5) working days. The manufacture and dispatch of the new Card may be invoiced in accordance with the Tariff Conditions applicable to the Cardholder and/or the payment account to which the Card is attached.

ARTICLE 7 - SEE THE SECRET CODE

This feature enables the Cardholder to view his or her Card PIN on the Mobile Application in real time. To be able to use this feature, the Cardholder must be equipped with the strong authentication device set up by the Issuer, to validate the viewing request. For security reasons, the Code is only visible for a few seconds. The Cardholder must authenticate again to view it again.

The Cardholder can view his or her PIN code on Mobile Application.