OPERATIONAL RULES

WHEREAS

The Merchant is bound by the terms and conditions set out herein and shall ensure that it complies with all operational rules in order for SlimPay to be able to properly deliver its services pursuant to the Contract signed by the Merchant with SlimPay. SlimPay shall inform the Merchant in the event of any changes to this document.

1. DEFINITIONS AND INTERPRETATION

Except as specifically stipulated to the contrary in any provision in which they should appear, the following terms and expression will have the meaning attributed to them below when written with initial capitals. Any other terms and expression with initial capitals not defined herein, shall have the meaning as set forth in the Contract with the Merchant.

1.1 ***Adobe Approved Trust List (or AATL)*** means the Adobe program that makes available an ensemble of electronic signature functions in PDF format allowing anyone receiving a document to verify its integrity and identify its author unequivocally with the Adobe Acrobat and Reader products starting with version 9.

1.2 ***Beneficiary*** means the beneficiary of the funds transferred using a Payment Order;

1.3 ***Certificate*** means an electronic file attesting to the link between the identity and the Public Key of the person holding the Certificate.

1.4 ***Certificate Authority (or CA)*** means one of the components of the Public Key Infrastructure (PKI) generating and issuing Certificates upon demand from the Registration Authority by applying the rules and practices determined by them in the associated Infrastructure Certificate Policy and Certification Practices Statement;

1.5 ***Certificate Policy*** means all of the rules announced and published by the CA describing the general characteristics of the Certificates it delivers. This document describes the obligations and responsibilities of the CA, the RA, the Certificate and all of the PKI components intervening in the entire life cycle of the Certificate. The Certificate Policies applicable to the Service on the signature date of this document are referenced in the special conditions to the Contract;

1.6 ***Certification Practices Statement*** means the statement of the practices used by a Certificate Authority to issue Certificates;

1.7 ***Currency*** means the currency of a member state of the European Economic Area that does not belong to the Eurozone

1.8 ***Data*** means the User data, information, publications and, generally, the data of the Merchant's database whose use is the subject of the Contract, which may be consulted only by the Merchant or persons placed under the Merchant's responsibility.

1.9 ***Day*** means a business day during which SlimPay and all service providers or intermediaries (such as Payment Method providerss) involved in a payment transaction conduct business to execute payment transactions. If a transaction is received or must be executed on a non-business interbank day, the transaction shall be declared received or to be executed on the next business interbank day;

1.10 ***Deadline*** means the deadline for receiving a Payment Order after which every Payment Order received is considered to have been received the following Day;

1.11 ***EEA*** European Economic Area

1.12 ***Electronic Signature*** means, in the terms of European Regulation 910/2014 (eIDAS), the use of a reliable process of identification guaranteeing its connection with the act to which it is attached and is intended to identify the person signing and manifesting the consent of the signatory to the obligations that arise from the document signed;

1.13 ***EPC*** means the European Payments Council. This is the decision-making and coordinating body of the European banking community in the field of payments;

1.14 ***EPC Rulebook*** is the SEPA payments rulebook as published by the EPC and available at the EPC website (www.europeanpaymentscouncil.eu);

1.15 ***Identification Procedure*** means the process of identifying users requesting Certificates, which is defined by the Merchant in accordance with the rules set forth in the Certificate Policy;

1.16 ***Incident*** means any repeated and reproducible defect occurring under normal use of the SlimPay Systems, exclusively attributable to the SlimPay Systems, and leading to the total or partial impossibility of benefiting from the functionalities provided in the Solution documentation, as referenced in the specific conditions of the Contract.

1.17 ***Mandate*** means A direct debit mandate, as defined by regulations, given by the User in its capacity as debtor to the Merchant in its capacity as creditor, on which:

- The User authorizes the Merchant to issue direct debit orders;
- The User authorizes its bank to debit its account in the amount of the orders presented;

1.18 ***Public Key*** means a mathematical key made public and which is used to verify the digital signature of a data received;

1.19 ***Public Key Infrastructure (PKI)*** means an ensemble of technical methods, people, documents and contracts to provide a secure environment for electronic exchanges with the help of asymmetric encryption systems. The PKI generates, distributes, manages and archives the Certificates;

1.20 ***Refund*** means the User's request to its payment service provider to reimburse the funds associated with the execution of a Payment Order after it is credited to the Merchant's Payment Account as the result of a dispute, or an unauthorised transaction that may result in a reversal by SlimPay in the Payment Account;

1.21 ***Registration Authority (or RA)*** means one of the PKI components approved by a CA to register, validate or reject requests for Certificates. This entity applies the Identification Procedure of users

requesting Certificates in accordance with the rules defined in the Certificate Policy;

1.22 ***Registration Office (or RO)*** means the Merchant, contact point between the User and the Registration Authority. The mission of this Office is to collect data on Users, possibly identification documents, and to verify in particular the link between a person's identity and his or her telephone number. This entity applies the Identification Procedure of users requesting Certificates in accordance with the rules defined by the Certificate Authority. The Registration Offices are under the responsibility of the Registration Authority, as are all of their actions. The Registration Authority has a duty to monitor and audit the Registration Offices;

1.23 ***Reject*** means the notification by the User's payment services provider or SlimPay of the impossibility of processing a Payment Order due to a technical problem;

1.24 ***Return*** means the decision of the User's payment service provider to refuse a Payment Transaction leading to its reversal by SlimPay;

1.25 ***SEPA*** means the Sole Euro Payment Area. The list of countries and territories of the SEPA area is available at the national SEPA committee website (www.sepafrance.fr);

1.26 ***Third-Party Archiver*** means a trusted entity that ensures and guarantees the durable conservation of electronic documents and the integrity of the restored information;

1.27 ***Time of Receipt*** means the Day on which SlimPay receives the Transfer Order initiated by the Merchant or any other Day subsequently agreed on (deferred execution Transfer Order) in accordance with these Operational Rules;

1.28 ***Trust File*** means all of the elements created during the generation of the transaction between the Merchant and the User, then kept for a period of time that conforms to the legal requirements as communicated by the Merchant permitting the traceability and existence of the execution of the transaction concluded in accordance with the procedures described in the TMP;

1.29 ***Trust Management Policy (TMP)*** means the document describing the technical processes used by the CA for the User to sign the document electronically, then the creation and maintenance of the Trust File during the use of the Service. On the signature date of this document, the applicable Trust Management Policy is referenced in the specific conditions of the Contract;

1.30 ***Trusted Third Party*** means an entity having received the accreditation of Electronic Certification Service Providers to implement electronic signatures within the architectures of the Public Key Infrastructures;

2. ELECTRONIC SIGNATURE

2.1 DESCRIPTION OF THE SERVICE. SlimPay makes available to the Merchant a service for registering User payment consents, capturing, controlling and filtering bank accounts, performing strong User authentication, signing a Mandate thanks to an Electronic Signature, managing and safeguarding Mandate data, archiving the Trust File, and materializing on demand the Trust File.

2.2 ROLES OF THE PARTIES. The Merchant acts as a Registration Office (RO) and SlimPay as the Registration Authority (RA). The Merchant can delegate under its full control and responsibility the Registration Office role to any other party.

2.3 REQUIREMENTS FOR ELECTRONIC SIGNATURE. The electronic Certificate associated with the Electronic Signature affixed to the document validated and accepted by the Merchant and the User complies with the X.509 standard ("ITU-T Recommendation X.509/ISO IEC 9594-8: 2001 "Information Technology - Open Systems Interconnection (OSI) - The Directory: Public-key and attribute certificate frameworks") and meets the requirement for an advanced Electronic Signature as defined by European Regulation 910/2014. The signed Mandate takes the form of a PDF file that encapsulates the signature Certificate duly recognized by the Adobe AATL mechanism or equivalent.

The Certificate is however not a qualified certificate. Therefore and in order to ensure the legal validity of the electronic signature affixed by the User, the Merchant is informed that it must be able, as needed, to justify the reliability of the process in accordance with article 26 of the European Regulation 910/2014. To this end:

(i) SlimPay agrees to assist the Merchant with such justification, by providing all of the elements ensuring the manifestation of the User's authorization, of the link between the signature and the instrument to which it is attached and of the general reliability of the SlimPay Services by making available all of the technical documents allowing verification of such reliability.

(ii) The Merchant agrees with SlimPay on a sufficient User Identification Procedure when the User Certificates are generated that allow the creation of the Electronic Signature. The implementation of these procedures shall be monitored regularly and periodically and may be audited by SlimPay in its capacity of Registration Authority.

(iii) The Merchant agrees with each User concerned on an explicit consent protocol by which the User gives its authorization to use its personal information for the purpose of delivering and keeping an electronic certificate for the on-line signature of a bank direct debit mandate.

(iv) It is recommended that the Merchant agree with the User that the electronic media constitute at least the beginnings of written evidence and that, in the event of dispute, the electronic documents produced by the SlimPay Systems shall prevail over those produced by the User, unless the latter demonstrates the lack of reliability or authenticity of the documents produced by the SlimPay Systems.

2.4 POWER OF EVIDENCE. The Merchant acknowledges that Electronic Signature legal effect and admissibility as evidence by the User's bank or in legal proceedings may be disputed if parts of the requirements that Merchant is responsible for are not executed. If the User's bank denies the Mandate validity on the ground of an insufficient resulting Electronic Signature evidence, the Payment transactions operated under this Mandate may be claimed by the User and shall be refunded by the

Merchant according to the Payment Scheme rules without prejudice to further Merchant's legal proceedings.

2.5 ARCHIVING. The Certificate Authority processes the data transmitted by the Merchant that are required to create a Trust File that will be associated with a given action or transaction. SlimPay will issue Certificates in accordance with the provisions of the applicable Certificate Policy and create Trust Files. The Certificate Authority complies with the provisions of the applicable Trust Management Policy and keeps it updated in accordance with the state of the art for information system security.

For the Trust File archival solution, and if it is part of the solutions provided as set forth in the specific conditions of the Contract, SlimPay archives and restores the Trust Files in accordance with the Trust Management Policy. An archive space, called a "safe", will be made available to the Merchant under the Contract and throughout its term to archive the Trust Files. Trust Files are archived for a period of ten (10) years after their creation and receipt by the provider of archiving services. The Third-Party Archiver shall create a system to notify the Merchant of the end of the archive period so that the Merchant can make the necessary decisions within a maximum period of sixty (60) days to extend the Trust File archiving period.

3. COLLECTION SERVICES

3.1 DESCRIPTION OF THE SERVICE. The Merchant may receive services such as acquisition of payment instruments, collection and settlement services (also referred to as full service solution). For this purpose, SlimPay will open a Payment Account in the name of the Merchant on which monies pursuant to Payment Transactions will be collected.

The Payment Account is held in euros unless otherwise explicitly requested by the Merchant in the special conditions, by indicating another Currency of a State that is a party to the European Economic Area. Any credit transactions denominated in a currency or currencies other than the currency of the Payment Account will be recognised and recorded in the Payment Account after conversion.

3.2 PAYMENT ACCOUNT. In accordance with Payment Services Directive (EU) 2015/2366 article 10, the funds received by SlimPay on behalf of the Merchant are safeguarded and consequently are credited to a segregated account opened specifically for this purpose by SlimPay through a first-tier partner bank that is duly approved by the French banking regulator.

The Net Balance of the Merchant's Payment Account is reproduced at any time on the bank accounts opened by SlimPay in the partner bank, namely the Merchant's funds deposited on the segregated account adjusted from the transactions of the Day associated with the Merchant's Payment Account which will be credited or debited in the segregated account no later than the end of the following Day.

4 TRANSACTION DEBITED TO THE PAYMENT ACCOUNT: TRANSFER ORDER

4.1 DESCRIPTION OF THE SERVICE. SlimPay executes Transfer Order to wireout Merchant's funds on its request to any bank account held by another payment service provider within EEA.

4.2 FORM OF ORDER. Merchant shall transmit Transfer Order to SlimPay exclusively in secured and signed electronic format. It shall contain the following elements: the amount, the due date, the unique identifier of the account to be credited, notwithstanding any other additional information such as the name of the Merchant or Beneficiary for example. If one or more unique identifications are incorrect, SlimPay is not responsible for the non-execution or incorrect execution of the Transfer Order. The Transfer Order must comply with the EPC Rulebook rules for SEPA payments or with the interbank rules of the local Payment Method used.

4.3 TIME OF RECEIPT AND IRREVOCABILITY. The Time of receipt of a Transfer Order is the date on which SlimPay confirms its receipt to the Merchant. The Time of receipt is the starting point of the period for execution of the transfer.

The Deadline for Transfer Orders reception is set as follows:

Order	Cut-off
SEPA credit transfer	08:00 CET

Transfer Orders are irrevocable as of the time they are placed in circulation in SlimPay's Payment system. After this date, no request to recall a Transfer Order by the Merchant in order to cancel it shall be receivable.

4.4 CONDITIONS OF EXECUTION. It is the responsibility of the Beneficiary's payment service provider to recognise the funds received in the account opened in the Beneficiary's name in accordance with the market rules applicable in this area.

The traceability of the movement of funds is ensured between SlimPay's bank and the Beneficiary's payment service provider by the uniques identifiers of the Payment Account of the Merchant and of the bank account of the Beneficiary.

4.5 DISPUTING A TRANSFER ORDER. Any dispute by the Merchant based on incorrect execution of the Transfer Order by SlimPay must be notified to SlimPay as soon as possible, and no later than five Days after the information given by SlimPay concerning the execution of the Transfer Order. After this period, no request from the Merchant shall be examined by SlimPay.

On the other hand, should this incorrect execution be caused by SlimPay's failure to perform its obligations under the Contract, SlimPay shall return the sums that should not have been debited.

Any Transfer Order that has not been duly authorised must be notified by the Merchant as soon as possible and no later than five Days after the information given by SlimPay concerning the execution of the Order. After this period, no request from the Merchant shall be examined by SlimPay.

5. TRANSACTIONS CREDITED TO THE PAYMENT ACCOUNT: PAYMENT ORDERS

5.1 DESCRIPTION OF THE SERVICE. SlimPay may acquire the following Payment Orders: SEPA Credit Transfer, direct debits or cards executed by the User's payment service provider according to the conditions on which they have agreed.
Payment Orders via direct debits and bank transfers in the SEPA and non-SEPA format may be acquired by SlimPay only if they are issued in euros or in the local currency of a party State to the EEA. The other categories of payment instruments that SlimPay may acquire are specified in the special conditions.
The amount of the Payment Orders acquired will be credited by SlimPay to the Merchant's Payment Account under the conditions stipulated below.

5.2 FORM OF ORDER. Merchant shall transmit Payment Order to SlimPay exclusively in secured and signed electronic format. It shall contain the following elements: the amount unless the Merchant agreed on a payment plan with SlimPay, the expected reception date of the funds, the unique identifier of the account to be debited or alternatively the token that SlimPay provided the Merchant to identify the User, notwithstanding any other additional information such as the name of the Merchant or User for example. If one or more unique identifications are incorrect, SlimPay is not responsible for the non-execution or incorrect execution of the Payment Order. The Payment Order must comply with the EPC Rulebook rules for SEPA payments or with the interbank rules of the local Payment Method used.

5.3 TIME OF RECEIPT AND IRREVOCABILITY. The Time of receipt of a Payment Order is for an immediate order the date on which SlimPay confirms its receipt to the Merchant and for a deferred order the date on which SlimPay confirms its implementation.The Time of receipt is the starting point of the period for execution of the payment.
The Deadline for Payment Orders reception is set as follows:

Order	Deadline
SEPA direct debit CORE	05:45 CET
SEPA direct debit B2B	05:45 CET

Payment Orders are irrevocable as of the time they are placed in circulation in SlimPay's Payment system. After this date, a Payment Order can be reversed on specific request of the Merchant following the Payment Scheme rules and subject to exceptional treatment costs. SlimPay will send the Merchant a proposal describing the terms (technical, financial, planning, etc.) of such reversal project. If agreed, this project will be the object of a specific order.

5.4 REJECT. The Merchant is informed that, before any credit to the Merchant's Payment Account, a transaction may be subject to a Reject by the User's payment service provider.

5.5 ACQUISITION PERIODS. The value date of the credit to the Merchant's Payment Account may not be later than the date of the Day on which SlimPay receives the funds associated with this payment transaction.
SlimPay credits the amount of the payment transaction to the Merchant's Payment Account immediately after its own account has been credited. This recognition is without prejudice to possible subsequent disputes or subsequent Refunds of the transaction and do not affect the related obligations of the Merchant.
SlimPay is not responsible for complying with the periods agreed on between the User and its payment service provider which may run between the date of receipt of the Payment Order by said provider and the date of receipt of the funds by SlimPay in its account opened by its bank partner.

5.6 TRANSACTION REVERSAL. If the amount credited to the Merchant's Payment Account by SlimPay has not been charged to the User's account by its payment service provider, for any reason, SlimPay must reverse the entry on the Merchant's Payment Account.

5.7 PROVISIONS SPECIFIC TO PAYMENT ORDERS VIA DIRECT DEBITS AND CARDS. The Merchant may recall a Payment Order by direct debit that has not yet been place in circulation in the Payment system by SlimPay's partner bank.
In the event of a Payment Order by direct debit or card, the User's payment service provider may itself issue a Return of the transaction pursuant to the applicable contractual conditions. In the case of a direct debit, the Return may be executed before D+X Days, D being the date of the initial debit from the User's account. X is specified by the Payment of the service used (X=5 for SEPA). SlimPay must reverse the transaction that has been refused in this manner.
In the case of a Payment Order by direct debit or by card in an amount unknown by the User at the time of consent, the Merchant recognises that the User may obtain from his payment service provider the Refund of the sums debited from under the conditions and within the periods they have agreed. The Refund then results in the Reversal by SlimPay of the entry previously booked to the Payment Account at the request of the User's payment service provider.

5.8 PROVISIONS COMMON TO ALL PAYMENT ORDERS.
In the case of an unauthorised Payment Order, the User's payment service provider may initiate a search for proof and obtain a Refund of the sums that were debited from the User's account. The Refund results in the Reversal by SlimPay of the entry previously booked to the Payment Account in accordance with the applicable regulations. SlimPay may cancel this Reversal if it proves that the User authorised the Payment Order.
In the case of Reversal, the Merchant recognises that it may not oppose execution or raise a dispute or claim against SlimPay. It is the Merchant's responsibility to contact the User, the User's payment service provider or any other third party, as applicable for any dispute or claim.

5.9 AMOUNT LIMITS ON PAYMENT AND TRANSFER ORDERS. The Merchant and SlimPay may agree on amount limits to Payment and Transfer Orders. These limits are defined in the special conditions of the Contract. However, SlimPay may unilaterally decide on a limit of the unit or cumulative amount of the Payment and/or Transfer Orders, beyond which Orders will be refused. SlimPay informs accordingly the Merchant by any means.

5.10 RELATED SERVICES. Exchange transactions are executed by SlimPay on the basis of the buy or sell price charged by the partner bank for the Currency in question on the date of receipt of the funds or of the issue of the Transfer Order, provided that it occurs before the Deadline specified in the special conditions of the Contract. If not, the rate of the next Day is applied. The foreign exchange risk due to rate fluctuations for the Currency in question is borne exclusively by the Merchant. SlimPay shall not under any circumstances be held liable.
In this respect, the Merchant declares that is has been informed by SlimPay and is fully informed of the exchange and rate risks related to the recognition or charging of any payment transaction or any Order denominated in a Currency other than the Currency of the Payment Account.

5.11 MERCHANT INFORMATION. SlimPay communicates a payment transaction reference to the Merchant for every Payment and Transfer Order. SlimPay provides real time access to data, allowing the Merchant to view the details of the credit and debit transactions on its Payment Account, the Payment Orders transmitted to SlimPay, the Transfer Orders executed by SlimPay and the status of these Payment Orders. This access allows the Merchant to consult all histories of payment transactions or histories for a given period and allows it to export data for its bank reconciliation or its account labelling.
In the event of a Payment Order credited to the Payment Account, the transaction reference is completed by a reference allowing the Merchant to identify the User, the amount and the time the Payment Order was received.
In the case of a Payment Order debited to the Payment Account, the transaction reference is completed by a reference allowing the Merchant to identify the Beneficiary, the amount and the time the Transfer Order was received.
The reference allowing identification of the User or Beneficiary is the unique identification number of his account with his payment service provider and any other reference associated with it under the special conditions of the Contract.
The fees relating to the acquisition of Payment Orders or the execution of Transfer Orders are denominated with notation of the transaction reference and the type of Payment or Transfer Order.

6 SERVICE LEVEL AGREEMENT

6.1 SCOPE THE SERVICE LEVEL AGREEMENT. The service level agreement concerns all SlimPay Systems except the archiving service that is subject to specific terms as described in article 7.

6.2 PRACTICAL TERMS AND HOURS. The SlimPay customer service contact information is as follows:
Email: support@slimpay.com
Or any update to this contact information as indicated on the web site support.slimpay.com.
Customer Service working hours are: From Monday through Friday, from 9am to 6pm, French time, working days.

6.3 GENERAL REQUEST PROCESSING.
For each request, the Merchant must provide the following information:
- Representative Name
- Telephone Number
- Request Details

In the case of an incident, additional information will be requested on the incident itself. SlimPay will send the Merchant a request number after receipt of the request. Information on how the request is processed will be recorded in a log.

6.4 PERFORMANCES AND RATE OF AVAILABILITY. SlimPay's commitments at the service level are subject to the Merchant's compliance with the operating conditions of the Service related to, in particular, the characteristics of the information transmitted.

6.5 RATE OF AVAILABILITY.
Access to the SlimPay Systems is available 24/7.
The availability rate of the SlimPay Systems is 99.5% on an annual basis.
The SlimPay Systems is said to be unavailable when it is the object of a level 1 incident.
The availability of the SlimPay Systems is defined by the responses received by SlimPay's monitoring tools to the requests issued from a web site or through the Application Programming Interface of the SlimPay Systems. Thus, the SlimPay Systems shall be considered available when it responds to the requests of SlimPay's supervision tools.
The following are specifically excluded from the availability rate calculation:
- Planned maintenance periods under the conditions mentioned below;
- Service interruptions resulting from the occurrence of an event of force majeure or an unforeseen accident as defined by the Contract;
- Service interruptions caused by the Merchant, in particular due to the non-conforming use of the Service and/or a use not authorized by SlimPay or to an Incident of the Merchant's IT system;
- Service interruptions caused by third parties, such as telecommunications or Internet bandwidth providers.

6.6 PERFORMANCE OF CERTIFICATE GENERATION SERVICES. The performance obligations of the Certificate generating solution refer to the period of availability.
These performance obligations are expressed in the processing times described below and are subject to the following conditions:
- The processing times exclude the transfer time between the User's workstation and the Trusted Third Party and exclude the execution of the signature mechanisms at the User's workstation.
- The "rate" is the number of requests that arrive at the certificate production units of the Trusted Third Party during a unit of time.
- The contractual rates listed below start with the principle that the instantaneous flow (number of requests per second) may not exceed 5 times the average contractual rate.

	Guaranteed processing times for 99% of requests	Maximum rate
	3 seconds	10,000

Verification of the user Code and generation of the certificate Delivery of an acknowledgment receipt		requests/day

Under the Contract, the maximum rate is 10,000 requests/day. However, if the Merchant reaches 8,000 requests/day, it will be possible to renegotiate the maximum rate of request/day through an amendment signed by a legal representative of the two Parties.

6.7 PERFORMANCE OF THE TRUST FILE MATERIALIZATION SERVICE. The processing time for the request for materialization or Trust Files is 7 working days as of the receipt of the request by SlimPay.

6.8 MAINTENANCE. An Incident means any repeated and reproducible defect occurring under the normal use of the SlimPay Systems, exclusively imputable to the SlimPay platform and leading to the total or partial impossibility of benefiting from SlimPay Systems.

6.9 CORRECTIVE MAINTENANCE. SlimPay provides the Merchant with a corrective maintenance service for the SlimPay Systems provided under the Contract in the conditions defined below.

6.10 DEFINITION OF THE LEVELS OF INCIDENT SEVERITY. The level of severity of an Incident is allocated by SlimPay and communicated to the Merchant after receipt of the incident notification.

Minor incident (severity 3) means any incident that affects the SlimPay Systems but allows the complete operations of the SlimPay Systems in all of its functionalities, even if through a workaround solution.

Major Incident (severity 2) means any incident impeding the operation of an essential functionality of the SlimPay Systems.

Blocking Incident (severity 1) means any incident rendering the use of the SlimPay Systems impossible in its entirety. A blocking incident is reported when it prohibits the implementation or use of the SlimPay Systems or when the repetition of a major incident becomes too restrictive for the Merchant.

6.11 TERMS FOR INCIDENT PROCESSING. Corrective maintenance occurs either by request from the Merchant via SlimPay customer-service or at SlimPay's initiative after identifying problems.

It is specified that, during non-working periods, incident detection is ensured by a monitoring system that notifies the standby personnel of incidents by text message:

- Technical supervision of infrastructures (memory, CPU, availability of SlimPay Systems or processes, etc.);
- Functional supervision (verification of the end-to-end operations on the basis of hourly testing.)

If the Merchant reports the occurrence of an Incident, it shall provide in writing (email, fax or mail) the following information:

- Description of the problem;
- Frequency of occurrence;
- Transaction number "Transnum";
- Name and version of the Internet browser used, if applicable;
- Computer and operating system used, if applicable.

When incidents occur that are documented by the Merchant or by SlimPay's operating teams and can be reproduced (program stoppage, program error, application error, memory violation, disk error, etc.), SlimPay will process these incidents as soon as possible according to the following procedure:

- Phase 1: Opening of an incident ticket notified to the Merchant by email
- Phase 2: Incident analysis and allocation of severity indicator notified to the Merchant by email
- Phase 3: Research for a definitive correction or a workaround solution if necessary
- Phase 4: Choice of the date of implementation of the workaround solution (immediate or deferred) based on the degree of severity
- Phase 5: Implementation of the definitive correction if available or, if applicable, implementation of a temporary workaround solution
- Phase 6: Incident closure

6.12 INCIDENT RESOLUTION DEADLINES. For Severity 1 Incidents, SlimPay implements continuous efforts until a solution is found and the Service is again functioning normally.

Severity	***Incident resolution deadlines***
Severity 1	4 hours during working periods and 8 hours during non-working periods
Severity 2	48 working hours
Severity 3	5 working days

The working period is defined in the paragraph "Practical Terms and Hours" of Article 6.2.

The time for resolving incidents starts when the incident has been qualified and recorded by SlimPay on the basis of elements communicated in writing by the Merchant and ends when the Service can be used by the Merchant in accordance with the commitments provided in this document, even if by a workaround solution.

The time for making the correction operational (start of production) is included in the processing time.

The correction or workaround for the incident will be made by SlimPay on the basis of:

- The set of messages and documents with the codes related to the incident;
- The description of the incident by the Merchant;
- The description of the context (conditions of occurrence, actions taken, etc.).

6.13 CORRECTIVE MAINTENANCE SCOPE OF APPLICATION. The scope of application of this maintenance is as follows:

- The platform and software constituting SlimPay Service;
- The services operated by the Trusted Third Party and the Third Party Archiver.

The following services are excluded from corrective maintenance:

- The correction of problems caused by a use of the SlimPay Systems or the software modules comprising the Service that do not conform to the associated user operations documentation;

- In the case of the use of third-party hardware or software that are not compatible with the SlimPay Systems or the software modules constituting the Service, except by prior written consent of SlimPay;
- Additions or modifications of the existing programs not required by a change to current regulations;
- Maintenance on one or more of the software applications other than the software modules under the Contract that operate in tandem with the latter;
- Modifications or additions to the functionalities pertaining to modifications made to the Merchant's hardware or software configuration.

These supplementary services will automatically be invoiced separately.

6.14 PREVENTATIVE MAINTENANCE. SlimPay will provide preventative maintenance services for the hardware and software comprising the SlimPay Systems so that they remain in good working order.
SlimPay will establish regular verifications in order to monitor the proper technical status and make any modifications to the SlimPay Systems it shall deem necessary to provide with a minimum of down time.
This preventative maintenance for the SlimPay Systems is performed in the form of a control analysis programmed and prepared by a maintenance technician. SlimPay shall keep the Merchant informed of the maintenance operations and their impact on the SlimPay Systems.
The Merchant is hereby notified that SlimPay's scheduled maintenance shall be performed on Thursdays from 9pm to 11pm. SlimPay will make its best effort to ensure the continuity of the SlimPay Systems and that it not be disturbed by the preventative maintenance performed by SlimPay. The Merchant shall be notified 2 weeks in advance of any maintenance operations outside of this maintenance range.

6.15 ONGOING MAINTENANCE. After consent from the Merchant on the financial and technical terms as applicable, SlimPay may perform ongoing maintenance to the SlimPay Systems platform either upon the express request of the Merchant, or by unsolicited proposal in the context of optimizing the quality of service and performance.

6.16 ACTIVITY REPORTING TERMS. SlimPay provides monitoring tools permitting the real-time reading and downloading of the reports on the time ranges chosen by the user. The monitoring tool is accessible via http://status.slimpay.com/

7 ARCHIVING SOLUTION SERVICE LEVEL AGREEMENT

7.1 SERVICE INCIDENT PROCESSING. If an Incident is identified in the archiving service, the Merchant will contact SlimPay's customer-service department as described in Article 6.2 and 6.3. SlimPay will process the identified Incidents with the Third Party Archiver and will inform the Merchant of the actions taken to resolve the Incidents.

7.2 SPECIFIC CONDITIONS FOR CLOSING AN ARCHIVING SERVICE INCIDENT. SlimPay may only declare an incident closed with respect to the Third Party Archiver if it has obtained the verbal or written confirmation of the Merchant, or in absence of such confirmation by the Merchant. SlimPay may declare the incident closed with the Third Party Archiver at the end of 5 working days in the case that the Merchant does not respond or does not collaborate in providing the information necessary to resolve the problem.

7.3 GUARANTY OF AVAILABILITY AND QUALITY OF SERVICE. The archiving service is guaranteed to operate 24/7. The time frame to reestablish the query function is 1 calendar day from the date of the Merchant's call.

7.4 MAINTENANCE. With a concern for the optimization and proper operation of the service, the Third Party Archiver reserves the right to interrupt the archiving service for maintenance purposes. In principle, these interruptions will take place, except for exceptional cases, from 12 am to 4 am for a maximum of eight times per month.
The Merchant shall be notified of any interruption by email as soon as possible for exceptional maintenance procedures and within 3 calendar days before the interruption due to maintenance.

8 TAKEOVER GUARANTY

SlimPay agrees to return to the Merchant all of the Data that belongs to it, in a format that is easily readable in an equivalent environment. Takeover applies as of the extinguishment of the Contract.

8.1 ITEMS TO BE TRANSFERED. Upon the effective date of the rescission of the Contract, for whatever reason, SlimPay shall make available to the Merchant, without expense to the latter:

- The hardware and/or software items made available to SlimPay by the Merchant to the extent that these items still exist upon the expiration or on the effective date of the termination of the Contract;
- The specific developments created under the Contract which are the Merchant's property;
- The Data on mass storage media.

8.2 FURTHER TECHNICAL ASSISTANCE. SlimPay agrees to explore the possibility for the Merchant to request supplementary services associated to the takeover and not included in the Contract price, such as the availability of additional means, training, preparing the target environment and potential startup support. In such case, SlimPay will send the Merchant a proposal describing the terms (technical, financial, planning, etc.) of such takeover project. If agreed, this project will be the object of a specific order.
The takeover process does not include the installation or provision of services at the Merchant's location, or any third party it designates, which shall remain its responsibility.

9 COMMUNICATION BETWEEN THE PARTIES

The Parties agree to exchange information in accordance with the following procedures:
For every request related to the services ***implementation***, please contact the on-boarding team at support@slimpay.com

For question or request related to operational execution of the Contract, please contact SlimPay ***customer service***
customer-service@slimpay.com
For every request for technical assistance, the Merchant may contact the ***technical support*** teams at support@slimpay.com
For every request for regulatory assistance, the Merchant may contact ***compliance*** and KYC teams at compliance@slimpay.com
For every request relating to billing, the Merchant may contact ***accounting*** teams at the following address: billing@slimpay.com

ANNEX 1

Identification Policy	Refer to the specific conditions of the Contract
Certificate Policy	SlimPay PC v1.1 dated 11/23/2010
Archiving Policy	SlimPay PA v1.1 dated 11/23/2010
Trust Management Policy	SlimPay PGP v1.1 dated 11/23/2010
Information System Security Policy	DT01 50 10 (PSSI)
Business Continuity Plan	DT01 60 10 (PUPA)
Functional Specifications of the SlimPay Systems	See API specification on SlimPay website

ANNEX 2

SLIMPAY MONITORING PROGRAM

The Merchant agrees to comply with the SlimPay Monitoring Program (SMP), designed to limit the Reversed transaction ratio of the Merchant.

CRITERIAS TO ENTER INTO THE SLIMPAY MONITORING PROGRAM

-Reversed transaction rate exceeding 10%;
-Return transaction rate exceeding 6%;
-Number of Reversed transactions exceeding 50;
-Number of Return transactions exceeding 30;
-Cumulative criteria and recorded for four (4) consecutive months. However, if the Reversed transaction rate exceeds unreasonably the thresholds above, SlimPay reserves the right to add the Merchant immediately into the SlimPay Monitoring Program.

STEP 1: TRIGGER (D-DAY TO D+4M)

The Merchant is reported as exceeding the thresholds see above relating to the number and rate of Reversed transaction (date D). It must stay in this exceeding position during four (4) months to enter into the SlimPay Monitoring Program (D+4M).
However, if the Reversed transaction rate exceeds unreasonably the thresholds above, SlimPay reserves the right to add the Merchant immediately into the SlimPay Monitoring Program (without the 4 months criteria).

STEP 2: OBSERVATION PERIOD (D+4M TO D+7M)

If the program is triggered, the Merchant enters a so-called observation period of three (3) months from the end of the four (4) month period (unless an immediate entry) in which the program triggers have been recorded.
SlimPay shall inform the Merchant by written notice of the entry into the SlimPay Monitoring Program, the duration, and the procedures for the exit of this Program.
This period of observation should allow the Merchant to reduce its monthly Reversed transaction rate to less than 10% or the number of monthly Reversed transactions you issue below fifty (50).

STEP 3: END OF THE OBSERVATION PERIOD

At the end of this period of three (3) months, if the Merchant fails to decrease the Reversed transaction rate or a number of monthly Reversed Transactions to a level lower than the thresholds defined above, SlimPay may suspend the processing and collection of new Transactions until the Merchant has taken appropriate measures in its respective systems or suspending any involved User(s).
SlimPay verifies and accepts them.

At this step, the observation period may end differently:

Case 1: The Reversed transactions rate and number are under the thresholds: in this case, the Merchant leaves the SlimPay Monitoring Program. SlimPay shall inform the Merchant by written notice to the Merchant of this exit.

Case 2: The Reversed transactions rate and number are still above the thresholds but the Merchant took an action plan validated by SlimPay: in this case, the Merchant leaves the SlimPay Monitoring Program to enter in a new Exit Observation Period of two (2) months (D+7M to D+9M).
If the Reversed transactions number or rate is still below the thresholds, the Merchant leaves the SlimPay Monitoring Program (go to Case 1).
If the Reversed transactions number or rate exceeds the thresholds again, the system of the second SlimPay Monitoring Program applies to the Merchant (go to Second SlimPay Monitoring Program).
SlimPay shall inform the Merchant by written notice to the Merchant.

Case 3: The Reversed transactions rate and number are still above the thresholds but the Merchant did not take an action plan: in this case SlimPay suspends the processing and collection of new Transactions until the Merchant has taken appropriate measures in its respective systems or suspending any involved User(s). SlimPay verifies and accepts them.
SlimPay informs the Merchant that he has fifteen (15) calendar days to submit an action plan to SlimPay.
If the action plan is validated, the Merchant enters the Observation Period of #2.
If the action plan is refused, the Merchant has fifteen (15) more calendar days to submit a valid action plan.
If the second action plan is refused, SlimPay notifies the immediate termination of the contract for default to remedy to a breach of obligation, according to the General Conditions of the Payment Services Contract.

Case 4: The Reversed transactions rate and number are still above the thresholds but the Merchant did not want to take an action plan: in this case SlimPay notifies the immediate termination of the contract for default to remedy to a breach of obligation, according to the General Conditions of the Payment Services Contract.

SECOND SLIMPAY MONITORING PROGRAM

If the program is triggered a second time for the Merchant, new measures are taken in addition of the previous measures. A second entry into the SlimPay Monitoring Program could trigger:

- Immediate termination of the contract for default to remedy to a breach of obligation, according to the General Conditions of the Payment Services Contract;
- Qualification of the Merchant performing a high-risk activity, which may entail the application of the pricing corresponding to the high-Risk activities;
- Penalty fees.