Acoustic Payments

This Service Description describes the SaaS Product referred to as Acoustic Payments. The applicable Order provides pricing and additional details. Terms not defined in this Service Description have the meaning given elsewhere in the Agreement.

1. Overview

1.1 Acoustic Payments

Acoustic Payments uses a PCI-compliant environment to connect to Customer systems to collect and process payment information from Customer's end customers.

Customers will have access to the following Acoustic Payments environments:

- Pre-production environment – for customer testing purposes, and
- Production environment – for live production processing

Included in the subscription fees for an Instance of the SaaS Product are the following:

a. Merchant Portal

b. Multiple project codes

c. Multiple countries and currencies

d. Multiple payment methods

e. Up to 2 Acquirers or third-party payment processors

f. Access to a test system

g. A base set of API services

Customers subscribing to an Instance of Acoustic Payments must also subscribe to API Payments and/or GUI Payments.

1.2 Optional Services

1.2.1 API Payments

API Payments are payment transactions that are processed via API calls directly from the Customer's systems using the Acoustic Payments API interface.

API Payments is a web services application programming interface, which is available in both XML and JSON formats. The SaaS Product includes supporting payment transaction services such as routing look-up service, cancellation/void services, 3D secure cardholder authentication services, payment captures, and settlement requests.

1.2.2 GUI Payments

GUI Payments are payment transactions that are initiated via one of the following Graphical User Interfaces provided by Acoustic Payments:

a) Hosted Payment Page – A ready-made payment GUI enabling a payer to enter and submit payment for a specific order or invoice.

b) Hosted Wallet Page – A ready-made wallet management GUI enabling an end user to store and maintain their payment information for a specific group of merchants.

c) Payment Link – A solution to collect payments via phone, chat, or mail without customer support agents touching sensitive payment data.

d) Merchant Portal – A web portal included with Acoustic Payments Instance that can be used to submit payment transactions.

The SaaS Product includes API services inside the GUI such as 3D secure cardholder authentication transactions, Payment Card Number (PAN) verification, gift card balance look-up, wallet updates, and hosted session status updates. If Customer configures GUI Payments Hosted Payment Page to authorize payment, any follow-on calls to Suppliers' Capture or Collect API services to request settlement of the authorized amount is included.

1.2.3 Token Transactions

Token Transactions includes the following two API services:

- Token Generation – Converts a Payment Card Number (PAN) into a token and returns the token to the requesting Customer. The generated token will be stored, unless already registred under the token group the Customer belongs to.
- Detokenize – Provides a detokenized card number encrypted with a public key provided by the Customer to ensure the intended recipient receives the card number.

Token Transactions can be initiated through direct API calls from Customer's applications or tokenization operations performed by Customer's used in Merchant Self-Service Portal. Token Transactions can also be performed as embedded operations in other transaction services such as but not limited to CardVerify, CardAuthroized, and CardAuthCap.

1.2.4 Data File Transactions

Data File Transactions provide API services to allows Customers to store, retrieve, search, and delete data files of voice recordings or images an end user mandates and payment authorizations with Acoustic Payments.

1.2.5 Additional Acquirers

Additional Acquirers allows Acoustic Payments to set up and support additional acquirers or third party payment processors.

1.2.6 Network Partners

Network Partners provides Acoustic Payments connections to service providers delivering additional payment support or value added services such as, but not limited to: payment gateways, payment service providers, fraud prevention service providers, and value added service providers.

1.2.7 Payment Reconciliation

Payment Reconciliation automatically matches settlement requests with payment funding information from acquirers and processors with a series of data feeds designed to automate A/R reconciliation, ledger postings, and cash application processes.

1.2.8 Data Warehouse

Data Warehouse delivers a near real-time data feed of Customer's transaction data to Customer's data warehouse.

1.3 Professional Services

1.3.1 Standard Implementation

Acoustic Payments Standard Implementation includes the following deliverables:

a. API keys for test and production
b. Customer set up on test and production systems:
    (1) 1 Project or Account Code
    (2) Up to 10 supported sales countries
    (3) Credit and debit card payment methods
    (4) Up to 2 pre-connected acquirers
    (5) Up to 5 user administrators on the Merchant Portal
c. Remote training via webinars for:
    (1) Secure Connectivity Setup
    (2) API implementation
    (3) Hosted Payment Page integration
    (4) Merchant Portal Administrators and Users
d. Email support for setup and test

1.3.2 Account Management

Acoustic Payments Account Management provides a named Account Manager who will provide mail and phone support to Customer that includes:

a. Daily operational support

b. Single focal point for change management, problem management, and event planning

c. Monthly business review and operational status meetings

Account Management Services will be delivered within normal business hours (09:00 – 16:00) based on the location of the appointed Account Manager.

1.3.3 Additional Services

Customers may purchase additional implementation and deployment support from Acoustic Payments as professional services sold on a Time & Material basis, using hourly rates, or on a fixed price basis.

2. API Services

Acoustic makes the following categories of services available to the Customer via API:

API Service Category	Suffix	Description	Charge Group
Payment transaction	POST /trx	Perform operations on card and alternative payment instruments, including but not limited to: Zero dollar authorization, Balance check, Credit check, Authorization, Incremental Authorization, Void, AuthCap, Voice Incremental Authorization, Voice Authorization, Voice AuthCap, Capture, Collect, Register Charge, Refund, Unrestricted Refund and Credit Transfer.	API Payments
Retrieving transaction data	GET /trx	Search and retrieve payment transaction data	Instance
3D-Secure	/s3d	3D Secure Cardholder Authentication using the Verified by Visa, MasterCard SecureCode, American Express SafeKey, JCB J-Secure and Diners/Discover ProtectKey facilities.	API Payments
Hosted GUI sessions	/ses	Create and retrieve Hosted Payment and Hosted Wallet Management sessions	GUI Payments
Card routing information	/cri	Check PAN, BIN and routing information for a specific card number	Instance
Transaction batches	/bat	Submit and retrieve responses for batches of payment transactions	Instance
Merchant notifications	/evt	Outbound notification to Client about payment status changes	Instance
Wallets	/pro	Create, update and retrieve user wallets	Instance
Token	/tkn /dtk	Tokenization and detokenization services to convert payment card numbers (PANs) into tokens, and vice versa.	Token
Data files	/dat	Storage and retrieval of data files	Data Files
Merchant payment routing	/rou	Setup and maintain payment routing setup	Instance
Payment device data	/pdd	Setup and maintain information about payment devices (terminals)	Instance
Merchant terminal ID	/pti	Setup and maintain merchant terminal IDs :	Instance

Reports	/rep	Setup report subscriptions	Instance
Ping	/ping	Check supplier system availability	Instance
Dynamic Currency Conversion	/dcc	Processing of DCC transactions to Acquirers	API Payments

3. Charges

3.1 Charge Metrics

The SaaS Product is available under the charge metric specified in the applicable Order. The following Charge Metrics apply to this SaaS Product:

- Instance means access to a specific configuration of the SaaS Product.
- Events mean the number of occurrences of a specific Event related to the use of the Acoustic Payments product.

  When acquiring Event entitlements for a SaaS Product, the following will be counted as an Event:

  (1) API Payments - Payment Authorization Requests or Credit Transactions. A Payment Authorization Request includes one call to a third party payment processor requesting authorization of a payment or a payment settlement request (Capture) when an authorization is not required. A Credit Transaction includes full or partial refunds of previous charges or credit transfers.

  (2) GUI Payments – Payment Authorization Requests submitted through a Hosted Payment Page, Hosted Wallet Page, Payment Link, or Merchant Portal.

  (3) Token Transaction – One call to either the token generation or detokentization API service

  (4) Data File Transactions – One call to store or retrieve a data file

  (5) Payment Reconciliation – One Capture or refund transaction sent to an acquirer for which the payment reconciliation services are performed.
- Engagement means a professional or training service related to the SaaS Product

3.2 Overages

If actual usage of the SaaS Product during the agreement period exceeds the stated Event entitlement specified in the applicable Order, the Customer will be charged for the overage as specified in the Order as applicable.

4. Security Description

4.1 Security Policies

Acoustic has an information security team and maintains privacy and security policies that are communicated to Acoustic employees. Acoustic requires annual privacy and security training for personnel. Acoustic security policies are revalidated annually based on industry practices and Acoustic business requirements. Security incidents are handled based on comprehensive incident response procedures. Acoustic maintains physical security standards designed to limit access to authorized personnel at Acoustic data centers, including limited and monitored access points. Visitors register upon entering and are escorted while on the premises.

4.2 Access Control

Acoustic authorized staff use two-factor authentication to an intermediate "gateway" management host. IP address blocking may be utilized to prevent access by known compromised Internet sites and users in U.S. embargoed countries. Access to Customer Data and transfer of data in or out of the hosting environment is logged. WIFI use is prohibited within the Acoustic data centers that support Acoustic Payments.

Acoustic Payments requires encryption of content during data transmission between the Acoustic network and Customer's network access point. The specific encryption methods are specified by contractual agreement with the Customer, and the encryption requires installation of SSL certificates at both Acoustic and Customer's sites. Only personal information required for the payment processing is collected. Acoustic Payments encrypts that content when at rest awaiting data transmission.

4.3 Service Integrity and Availability

Modifications to operating systems, application software, and firewall rules are handled under Acoustic's change management process. Changes to firewall rules are reviewed by the Acoustic security staff before implementation. Acoustic monitors the data center 24x7. Internal and external vulnerability scanning is conducted regularly by authorized administrators and third-party vendors to help detect and resolve potential system security exposures. Malware detection systems (antivirus, intrusion detection, vulnerability scanning, and intrusion prevention) are used in all Acoustic data centers. Acoustic's data center services support a variety of information delivery protocols for transmission of data over public networks. Examples include HTTPS/SFTP/FTPS/S/MIME and site-to-site VPN. Backup data intended for off-site storage is encrypted prior to transport.

4.4 Activity Logging

Acoustic maintains logs of its activity for systems, applications, data repositories, middleware and network infrastructure devices that are capable of and configured for logging activity. To minimize the possibility of tampering and to enable central analysis, alerting and reporting, activity logging is done in real-time at central log repositories. Data is signed to prevent tampering. Logs are analyzed in real-time and via periodic analysis reports to detect anomalous behavior. Operations staff is alerted to anomalies and contacts a 24x7 on-call security specialist when needed.

4.5 Compliance

Acoustic performs industry standard ISAE3402 audits (or their equivalent) annually in production Payments data centers for compliance with Acoustic information security policies. Acoustic's annual PCI DSS certification includes on-site audits by external Qualified Security Assessor (Trustwave) in all Payments data centers. The Attestation of Compliance (AoC) or Compliance Letter is available to Customer and its auditors upon request.

4.6 Statement of Security Practices

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside Customer's enterprise. Improper access can result in information being altered, destroyed, or misappropriated or can result in misuse of Customer's systems to attack others. Without a comprehensive approach to security, no IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. Acoustic systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products, or services to be most effective. Acoustic does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

4.7 Personal Information and Regulated Content

Acoustic Payments will enable Customer to input and manage content containing the following information which may be considered personal or sensitive information pursuant applicable privacy laws:

- Contact information, including name, address, phone number, email address
- End-customer payment credential information

The communication, storage, and use of the above data is governed and audited on a yearly basis to conform with Payment Card Industry – Data Security Standards (PCI-DSS).

5. Service Levels

5.1 Service Level Agreement

Acoustic provides the Customer with the following availability service level agreement (SLA). Acoustic will apply the highest applicable compensation based on the cumulative availability of the SaaS Product as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact Acoustic regarding service availability issues are in Acoustic's SaaS support overview at acoustic.com/acoustic-terms/.

Availability during a contracted month	Compensation (% of monthly subscription fee* for contracted month that is the subject of a claim)
< 99.99%	2%
< 99.80%	4%
< 99.60%	6%
< 99.30%	8%
< 99.00%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

5.2 Response Time Service Level Agreements

Acoustic offers two response time SLAs as follows:

a. **Median API Response Time**

The median Acoustic response time for CheckoutStartSession and CardAuthorize web services will be less than 100 milliseconds.

The Acoustic response time for a given web service is measured as the elapsed time from when the web service request is received at the entry point to Acoustic's system, until Acoustic's web service response is sent back to Customer, minus any time Acoustic's system has spent waiting for responses from downstream third-party processors.

The service level target is calculated as the median Acoustic response time for CheckoutStartSession and CardAuthorize web services respectively across all such web service requests in a given month.

Median Response Time (during a contracted month)	Compensation (% of monthly subscription fee* for contracted month that is the subject of a claim)
> 100 ms	2%
> 500 ms	6%
> 1 second	10%

b. **99% Response Time**

99% of CheckoutStartSession and CardAuthorize web services will have an Acoustic response time of less than 1 second.

The Acoustic response time is calculated the same as defined above for the median Acoustic web service response time.

The service level target is calculated as the 99 percentile Acoustic response time for CheckoutStartSession and CardAuthorize web services respectively across all such web service requests in a given calendar month.

99% Response Time (during a contracted month)	Compensation (% of monthly subscription fee* for contracted month that is the subject of a claim)
> 1 second	2%
> 5 seconds	6%
> 10 seconds	10%

5.3 Additional Service Level Information

Service Level Agreements are available to the Customer and do not apply to claims made by an end user or for any beta or trial services. The SLA does not apply to any non-production environments including, but not limited to, test, disaster recovery, quality assurance, or development.

Acoustic will not process claims against a Response Time SLA when an availability service level outage has been recorded for the same period of time.

5.4 Service Level Objective

The following service level objectives are a goal and do not constitute a warranty to Customer. There is no refund, credit, or remedy available to Customer in the event Acoustic does not meet the service level objectives.

Service	Objective
Batch Processing Turn-Around-Time	90% of all transaction batches will be processed to completion in less than 60 minutes from receipt.
E-Mail Responsiveness	95% of e-mail sent to Acoustic's shared support mailbox will be answered within 24 business hours.
24x7 Help Desk Call Answer Response Tim4e	Acoustic's 24x7 Help Desk will answer phone calls in less than 60 seconds.
Security Management	● Acoustic acknowledges responsibility for the security of the Customer's cardholder data processed and will renew Acoustic's PCI-DSS Level 1 Certification at least once per annum. ● Acoustic will remediate High severity security vulnerabilities within 10 days. ● Acoustic will remediate Low severity security vulnerabilities within 30 days.
Pre-Production system availability	● Available for client testing 24x7 ● Pre-Production system is unattended outside normal Central European work hours. ● Pre-Production system incidents will, by default, be handled as severity 3.