PAYMENT SECURITY POLICY

Security Capabilities & Card Data Transmission Notice

CALLINGFANS PLATFORM

www.callingfans.com

Document Classification:	Public — Payment Processor Compliance Reference
Document Type:	Payment Security Policy / Card Data Transmission Notice
Prepared For:	CCBill Underwriting / Visa-Mastercard Compliance / Acquiring Banks
Payment Processors:	Stripe / PayPal (Third-Party PCI-DSS Compliant Processors)
Card Data Stored by Platform:	None — Zero cardholder data retained by CallingFans
Security Standard:	PCI-DSS Compliant via Third-Party Processor Delegation
Compliance Contact:	info@callingfans.com

This document sets forth the payment security architecture, card data handling practices, and third-party processor delegation model of CallingFans. It is prepared for review by payment processors, acquiring banks, card networks, and compliance departments.

TABLE OF CONTENTS

1. SCOPE AND PURPOSE

This Payment Security Policy (**"Policy"**) describes the security capabilities, card data handling practices, and payment processing architecture of the CallingFans platform (**"Platform"**), operated by **ONLY4FITNESS LTD** and accessible at www.callingfans.com.

This Policy is published in accordance with the requirements of card networks (Visa and Mastercard), payment processor compliance standards (including CCBill), and applicable data security regulations including the Payment Card Industry Data Security Standard (**"PCI-DSS"**). It is intended to provide acquiring banks, payment processors, and compliance reviewers with a clear and accurate description of how payment card data is handled in connection with transactions processed through the Platform.

This Policy applies to all payment transactions initiated by users (**"Fans"**) to purchase content, subscriptions, or services offered by Creators on the Platform, regardless of the payment method selected.

2. CORE SECURITY DECLARATION — NO CARD DATA RETENTION

AFFIRMATIVE SECURITY DECLARATION: CallingFans does not collect, store, process, or retain any payment card information. This includes, without limitation, full card numbers (PAN), card expiration dates, card security codes (CVV/CVC/CVV2), cardholder names in isolation, or any other Sensitive Authentication Data (SAD) as defined under PCI-DSS. All payment card data is handled exclusively by PCI-DSS compliant third-party payment processors.

This declaration is the foundational principle of the Platform's payment security architecture. By routing all cardholder data entry and processing through certified third-party payment processors, CallingFans effectively removes itself from PCI-DSS scope with respect to cardholder data storage, processing, and transmission.

3. PAYMENT PROCESSING ARCHITECTURE

a. Third-Party Processor Model

CallingFans operates a **third-party processor delegation model** for all payment transactions. Under this model, the Platform does not directly handle, transmit, or store payment card data at any stage of the transaction lifecycle. All cardholder data entry occurs on the secure, PCI-DSS certified infrastructure of the applicable third-party payment processor.

This architecture is deliberately designed to minimize the Platform's exposure to cardholder data and to ensure that payment security obligations are fulfilled by dedicated, certified payment security specialists.

b. Supported Payment Processors

CallingFans currently supports the following PCI-DSS certified third-party payment processors:

Processor	Certification	Data Handling	Cardholder Data Scope
Stripe	PCI-DSS Level 1 Service Provider	All card data entered directly on Stripe infrastructure	Stripe — not CallingFans

PayPal	PCI-DSS Level 1 Service Provider	All card data entered directly on PayPal infrastructure	PayPal — not CallingFans

c. Checkout Flow and Data Routing

The payment checkout flow is designed to ensure that cardholder data never transits through the Platform's own servers. The process operates as follows:

Step	Action	Where Data Is Processed
1	User selects content or subscription and proceeds to checkout	CallingFans Platform
2	User is redirected to the secure payment page of the selected processor (Stripe or PayPal)	Processor's PCI-DSS Environment
3	User enters payment card details directly on the processor's secure interface	Processor's PCI-DSS Environment
4	Processor authorises the transaction and returns a secure token to CallingFans	Processor's PCI-DSS Environment
5	CallingFans receives only the secure token — no card data — and fulfils the order	CallingFans Platform

4. PCI-DSS COMPLIANCE FRAMEWORK

a. Platform PCI-DSS Scope

By virtue of the third-party processor delegation model described in Section 3, the CallingFans Platform operates outside the scope of PCI-DSS with respect to the storage, processing, and transmission of cardholder data. The Platform does not:

- Accept, capture, store, or transmit full Primary Account Numbers (PAN).
- Store, process, or transmit card expiration dates, security codes (CVV/CVC/CVV2), or PINs.
- Operate any system or interface through which cardholder data transits.
- Maintain any database, log file, or record containing Sensitive Authentication Data (SAD).

b. Processor PCI-DSS Responsibility

All PCI-DSS obligations with respect to the storage, processing, and transmission of cardholder data are borne by the applicable third-party payment processor (Stripe or PayPal). Both processors maintain PCI-DSS Level 1 Service Provider certification — the highest level of PCI-DSS compliance — and are responsible for the security of all cardholder data within their respective environments.

c. Tokenization Model

Upon successful completion of a payment transaction by the processor, the Platform receives a **secure payment token** in lieu of cardholder data. This token:

- Is a non-sensitive reference identifier generated and issued by the payment processor.
- Does not contain, encode, or allow derivation of any cardholder data.
- Is used solely for the purpose of referencing the transaction within the Platform's systems.

- Cannot be used to initiate, reverse, or modify payment transactions without authorisation from the issuing processor

TOKENIZATION CONFIRMATION: CallingFans does not store full card numbers, expiration dates, or security codes at any point. The only payment-related data retained by the Platform from the processor is a secure token, together with: the card type, the first two and last four digits of the card number (where provided by the processor), and — where applicable — the cardholder's name and email address as provided by the processor. No further cardholder data is retained.

5. DATA TRANSMISSION SECURITY

a. Encryption in Transit

All data transmitted between users and the CallingFans Platform is encrypted in transit using industry-standard Transport Layer Security (**TLS**) protocols. The Platform enforces HTTPS across all pages and endpoints, ensuring that no data is transmitted over unencrypted connections.

All data transmitted between the Platform and third-party payment processors is similarly encrypted using TLS, in accordance with the processors' own security standards and PCI-DSS requirements.

b. Secure Checkout Redirection

At the final stage of the checkout process, the user is directed to the secure, hosted payment page operated by the applicable third-party processor (Stripe or PayPal). This page is served entirely from the processor's own PCI-DSS certified infrastructure. At no point during the card data entry stage does the user's browser transmit card data to any CallingFans server or endpoint.

c. Data the Platform Receives from Processors

Following completion of a payment transaction, the Platform receives only the following limited, non-sensitive information from the payment processor:

Data Element	Description	Cardholder Data?
Payment Token	Unique processor-generated reference for the transaction	No
Card Type	Card network (e.g., Visa, Mastercard)	No
Partial Card Number	First two and last four digits only (e.g., 40** **** **12)	No
Card Expiry (partial)	Month and year only — not full expiry	Minimal
Cardholder Name	Where provided by the processor to the Platform	Yes — limited
Email Address	Where provided by the processor to the Platform	Yes — limited
Transaction Status	Authorised / declined / pending	No

6. CARDHOLDER DATA — WHAT CALLINGFANS DOES NOT STORE

For the avoidance of doubt, and for the express benefit of acquiring banks, payment processors, and compliance reviewers, CallingFans affirms that it does not store, log, cache, or retain any of the following data elements at any time:

Data Element	PCI-DSS Classification	Stored by CallingFans?
Full Primary Account Number (PAN)	Cardholder Data	**NO**
Card Expiration Date (full)	Cardholder Data	**NO**
CVV / CVC / CVV2 / CID Security Code	Sensitive Authentication Data (SAD)	**NO**
PIN / Encrypted PIN Block	Sensitive Authentication Data (SAD)	**NO**
Magnetic Stripe Track Data	Sensitive Authentication Data (SAD)	**NO**
Chip Data (ICC / EMV)	Sensitive Authentication Data (SAD)	**NO**

7. FRAUD PREVENTION AND TRANSACTION MONITORING

CallingFans employs a multi-layered approach to fraud prevention and transaction monitoring, in conjunction with the built-in fraud detection capabilities of its third-party payment processors:

- **Processor Fraud Detection** — Stripe and PayPal operate advanced, real-time fraud detection systems including machine learning-based risk scoring, velocity checks, and card network fraud tools (e.g., Visa Advanced Authorization, Mastercard Safety Net).
- **Identity Verification** — All Creators are required to complete identity verification prior to receiving payments. This reduces the risk of fraudulent account creation and unauthorized payout requests.
- **Access Controls** — The Platform enforces two-factor authentication (2FA) for account access, reducing the risk of unauthorized account takeover.
- **Transaction Monitoring** — Unusual transaction patterns are monitored and flagged for review in accordance with the Platform's internal compliance procedures.
- **Chargeback Monitoring** — The Platform actively monitors chargeback rates and takes corrective action where necessary to maintain compliance with card network thresholds.

8. INCIDENT RESPONSE AND BREACH NOTIFICATION

In the event of a suspected or confirmed security incident affecting payment data or user personal data, CallingFans maintains the following incident response commitments:

- **Immediate Containment** — Upon identification of a security incident, the Platform will take immediate steps to contain and mitigate the impact.
- **Processor Notification** — Where a security incident may affect payment processing, the applicable third-party processor(s) will be notified promptly in accordance with their incident response requirements.
- **Regulatory Notification** — Where required by applicable law (including GDPR and national data protection legislation), the Platform will notify the relevant supervisory authority within the prescribed timeframe.

- **User Notification** — Where a security incident is likely to result in a high risk to the rights and freedoms of affected users, those users will be notified without undue delay.
- **Post-Incident Review** — Following resolution of a security incident, the Platform will conduct a post-incident review and implement remediation measures as appropriate.

NOTE: Because CallingFans does not store, process, or transmit full cardholder data, the risk of a payment data breach originating from the Platform's own infrastructure is substantially mitigated. Any breach affecting cardholder data would be the responsibility of the applicable third-party payment processor, which maintains its own incident response and breach notification procedures.

9. THIRD-PARTY PROCESSOR SECURITY STANDARDS

CallingFans relies on the following third-party payment processors, each of which maintains industry-leading security certifications and compliance programmes:

Attribute	Stripe	PayPal
PCI-DSS Level	Level 1 Service Provider	Level 1 Service Provider
Encryption	TLS 1.2+ / AES-256	TLS 1.2+ / AES-256
Tokenization	Yes — Stripe Tokens	Yes — PayPal Tokens
3D Secure	Supported (3DS2)	Supported (3DS2)
Fraud Detection	Stripe Radar (ML-based)	PayPal Fraud Protection
Data Residency	Multi-region (US/EU)	Multi-region (US/EU)
Privacy Compliance	GDPR / CCPA	GDPR / CCPA

CallingFans conducts periodic reviews of its third-party payment processor relationships to ensure continued compliance with applicable security standards. The Platform reserves the right to add or modify payment processor relationships subject to compliance review and user notification, in accordance with its Privacy Policy and Terms of Service.

10. CONTACT AND COMPLIANCE INQUIRIES

For any inquiries relating to this Payment Security Policy, the Platform's payment security architecture, or PCI-DSS compliance matters, please contact us using the information below.

General Compliance Inquiries	info@callingfans.com
Payment Security Questions	info@callingfans.com	Subject: Payment Security
Legal Entity	ONLY4FITNESS LTD

Registered Address	Dean Street, London W1D 1PT, England
Platform Website	www.callingfans.com
Payment Security Page URL	www.callingfans.com/p/payment-secure
Supported Processors	Stripe · PayPal

CallingFans — Payment Security Policy & Card Data Transmission Notice
Prepared for CCBill underwriting, Visa/Mastercard compliance, and acquiring bank review.
Operator: ONLY4FITNESS LTD | www.callingfans.com