RAILS CLOUD

Rails Pay

PCI-DSS Alignment Statement

Payment Card Industry Data Security Standard — Current Posture and Roadmap

Version	Date	Classification	Standard
1.0	**March 2026**	**CONFIDENTIAL**	**PCI-DSS v4.0**

IMPORTANT This document describes Rails Pay's current alignment with PCI-DSS v4.0 requirements and the roadmap to full certification. It is provided for due diligence purposes. Full PCI-DSS certification is a target milestone — see Section 7 for the roadmap. This document does not constitute a formal PCI-DSS attestation of compliance (AOC).

1. Overview of Rails Pay and Payment Processing

Rails Pay is the payment infrastructure product of Rails Cloud, providing multi-currency digital wallets, payment aggregation, and merchant payment acceptance for businesses operating in and across Africa. Rails Pay processes transactions denominated in USD, ZAR, and ZiG (Zimbabwe Gold).

As a payment platform handling cardholder data and facilitating payment card transactions, Rails Pay operates within the scope of the Payment Card Industry Data Security Standard (PCI-DSS). Rails Cloud takes its obligations under PCI-DSS seriously and is actively implementing a structured compliance programme aligned to PCI-DSS version 4.0 (published March 2022).

RAILS PAY SCOPE Rails Pay currently operates as a payment facilitator and wallet provider. Card-present transactions are not in scope at this stage. The current scope covers card-not-present (CNP) transactions, digital wallet funding, and inter-wallet transfers across the Rails Pay network.

2. Understanding PCI-DSS

2.1 What is PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) is a global security standard established by the PCI Security Standards Council (PCI SSC) — a body founded by American Express, Discover, JCB, Mastercard, and Visa. It defines the security requirements for organisations that store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD).

2.2 PCI-DSS v4.0 Requirements Framework

PCI-DSS v4.0 is organised into 12 top-level requirements across 6 goals:

Goal	Requirements
Build and maintain a secure network and systems	Req 1: Install and maintain network security controls. Req 2: Apply secure configurations to all system components.
Protect account data	Req 3: Protect stored account data. Req 4: Protect cardholder data with strong cryptography during transmission.
Maintain a vulnerability management programme	Req 5: Protect all systems against malware. Req 6: Develop and maintain secure systems and software.
Implement strong access control measures	Req 7: Restrict access to system components by business need. Req 8: Identify users and authenticate access. Req 9: Restrict physical access to cardholder data.
Regularly monitor and test networks	Req 10: Log and monitor all access to system components and cardholder data. Req 11: Test security of systems and networks regularly.
Maintain an information security policy	Req 12: Support information security with organisational policies and programmes.

2.3 Merchant Level and SAQ Applicability

Rails Pay's merchant level and applicable self-assessment questionnaire (SAQ) are determined by annual transaction volume and processing method. Rails Pay currently operates as a Level 4 merchant by volume, with applicability to SAQ A-EP (e-commerce merchants using third-party payment pages with script-based interaction). As transaction volumes grow and the platform matures, Rails Cloud is targeting Level 2 merchant formal assessment.

3. Current PCI-DSS Alignment Posture

The following table sets out Rails Pay's current alignment status against each of the 12 PCI-DSS v4.0 requirements. Status definitions:

Implemented	Controls meeting this requirement are fully deployed and operational in production
In Progress	Work actively underway — partially deployed or pending final validation
Planned	Scheduled in the compliance roadmap with a defined target date

Req	Title	Status	Rails Pay Implementation Detail
1	**Network Security Controls**	**Implemented**	VPC isolation, security groups with default-deny posture, WAF deployed. Network segmentation separates cardholder data environment (CDE) from general infrastructure.
2	**Secure Configurations**	**Implemented**	CIS benchmarks applied to all CDE components. Default credentials changed on all systems. Configuration hardening documented and reviewed quarterly.

Req	Title	Status	Rails Pay Implementation Detail
3	**Protect Stored Account Data**	**Implemented**	Rails Pay does not store full PANs, CVVs, or magnetic stripe data. Tokenisation used for all card references. Stored data limited to truncated PANs and expiry dates where required for dispute management.
4	**Cryptography in Transit**	**Implemented**	TLS 1.2 minimum enforced on all cardholder data transmission. TLS 1.3 preferred. Certificate pinning implemented in the Rails Pay mobile SDK. No unencrypted transmission of cardholder data permitted.
5	**Protection Against Malware**	**Implemented**	Anti-malware deployed on all applicable CDE components. Real-time scanning with automated alerting. Dependency scanning on all Rails Pay application code.
6	**Secure Systems and Software**	**In Progress**	SDLC security controls implemented including code review requirements and SAST tooling. Penetration testing of payment flows in progress. Web application firewall protecting payment endpoints. Formal SDLC policy documentation pending completion.
7	**Restrict Access by Business Need**	**Implemented**	RBAC enforced on all CDE access. Role definitions documented. Minimum access principle applied. Access provisioning requires approval workflow.
8	**Identify and Authenticate Users**	**Implemented**	Unique IDs for all CDE users. MFA mandatory for all privileged CDE access. Password complexity and rotation policies enforced. Shared accounts prohibited in CDE.
9	**Restrict Physical Access**	**Implemented**	CDE hosted on AWS infrastructure with ISO 27001 / SOC 2 physical security. No Rails Cloud owned physical CDE. AWS physical security documentation available at aws.amazon.com/compliance.
10	**Logging and Monitoring**	**Implemented**	All CDE access logged with user, timestamp, IP, and action. Logs stored in write-once, tamper-evident storage. Real-time alerting on suspicious CDE activity. Log retention minimum 12 months.
11	**Regular Security Testing**	**In Progress**	Quarterly internal vulnerability scans conducted. Third-party penetration test of payment flows scheduled Q2 2026. ASV external scanning programme being established. File integrity monitoring in deployment.
12	**Information Security Policy**	**In Progress**	Security policies documented (see Rails Cloud Security Overview). PCI-specific policy amendments in progress. Annual security training programme being formalised. Incident response plan updated to include PCI breach notification procedures.

4. Cardholder Data Environment (CDE) Scope

4.1 What Rails Pay Stores

Rails Pay has implemented a minimisation strategy to reduce PCI-DSS scope. The following table describes what cardholder data Rails Pay does and does not store:

Data Element	Stored?	Detail
Primary Account Number (PAN)	Truncated only	Last 4 digits only, for display purposes. Full PAN never stored.
Cardholder Name	Yes (encrypted)	Stored encrypted for KYC and dispute management. Not accessible to application layer in plaintext.
Service Code	No	Not stored.
Card Expiry Date	Yes (encrypted)	Required for transaction validity checks. Stored encrypted alongside tokenised card reference.
CVV / CVV2 / CVC2	Never	Never stored post-authorisation. Prohibited by PCI-DSS. Immediately discarded after transaction processing.
PIN / PIN Block	Never	Card-present PIN transactions are out of Rails Pay's current scope.
Magnetic stripe / chip data	Never	Card-present transactions not currently in scope.
Card token (network token)	Yes	Network tokens issued by card schemes used in lieu of PAN for recurring transactions. Tokens are not cardholder data.

4.2 Tokenisation Strategy

Rails Pay uses a dual tokenisation strategy to minimise cardholder data exposure:

1. Network tokenisation: card scheme-issued network tokens (Visa Token Service, Mastercard MDES) replace PANs for recurring and stored-credential transactions, reducing PCI scope.
2. Payment processor tokenisation: for card-not-present transactions, card details are passed directly to the payment processor's hosted fields — they never transit through Rails Cloud servers. The processor returns a processor-specific token stored in the Rails Pay vault.

This architecture means that Rails Pay's CDE scope is limited to the token vault, transaction records, and the secure communication channels between Rails Pay and payment processors.

5. Rails Pay Merchant Obligations

Merchants and businesses using Rails Pay to accept card payments have their own PCI-DSS compliance obligations. The extent of these obligations depends on how they integrate Rails Pay:

Integration Method	Merchant PCI Scope	Applicable SAQ
Rails Pay hosted payment page (full redirect)	Minimal — merchant never touches cardholder data	SAQ A (simplest)
Rails Pay embedded JavaScript (hosted fields)	Reduced — JS renders in merchant page but data goes directly to Rails Pay	SAQ A-EP
Rails Pay API (direct integration)	Full scope — merchant transmits cardholder data via API	SAQ D or full QSA assessment
Rails Pay mobile SDK	Reduced — SDK handles cardholder data capture	SAQ A-EP (mobile equivalent)

Rails Cloud strongly recommends that merchants use the hosted payment page or embedded JavaScript (hosted fields) integration to minimise their own PCI-DSS scope. Rails Cloud provides documentation on PCI-DSS merchant responsibilities at docs.railscloud.co/rails-pay/pci.

6. American Express Integration and Compliance

Rails Pay is pursuing an American Express enablement partnership through Nedbank. As part of this partnership, the following Amex-specific compliance obligations are being addressed:

6.1 Amex SafeKey (3D Secure)

Rails Pay is implementing support for American Express SafeKey (Amex's 3D Secure 2.0 implementation) for all card-not-present Amex transactions. SafeKey provides an additional layer of fraud protection and shifts chargeback liability to the card issuer for authenticated transactions.

6.2 Amex Data Security Operating Policy (DSOP)

American Express requires all partners and merchants to comply with the Amex Data Security Operating Policy (DSOP), which aligns with PCI-DSS but includes Amex-specific requirements. Rails Pay's compliance programme explicitly covers DSOP requirements and these are tracked alongside the PCI-DSS requirements matrix above.

6.3 ISV Programme Requirements

As Rails Cloud pursues ISV (Independent Software Vendor) registration with American Express, the following additional compliance requirements are being addressed:

- Amex ISV programme registration and annual recertification
- SafeKey 2.0 implementation validation
- Fraud monitoring and chargeback management reporting to Amex standards
- Amex transaction data handling in accordance with DSOP

7. PCI-DSS Certification Roadmap

Rails Cloud is committed to achieving formal PCI-DSS certification for Rails Pay. The following roadmap sets out the key milestones:

Target Date	Milestone	Detail
Q2 2026	SAQ A-EP Completion	Complete and submit Self-Assessment Questionnaire A-EP for current Rails Pay e-commerce processing scope. Internal review and gap remediation.
Q2 2026	ASV Scanning	Engage Approved Scanning Vendor (ASV) for quarterly external vulnerability scans of CDE-connected IP ranges.
Q3 2026	Penetration Test	Third-party PCI-scoped penetration test of Rails Pay CDE and payment flows. Remediate all critical and high findings.
Q3 2026	SafeKey 2.0 Live	American Express SafeKey 2.0 (3DS) fully implemented and validated for all Amex CNP transactions on Rails Pay.
Q4 2026	Level 2 Assessment	Engage Qualified Security Assessor (QSA) for Level 2 merchant assessment as transaction volumes qualify. Target formal AOC issuance.
Q1 2027	Formal AOC	Receive and publish Attestation of Compliance (AOC) for PCI-DSS v4.0. Provide AOC to Amex, Nedbank, and enterprise customers on request.

8. Shared Responsibility for PCI Compliance

PCI-DSS compliance is a shared responsibility between Rails Cloud and merchants using Rails Pay. The following responsibilities apply:

Rails Cloud Responsible For	Merchant Responsible For
Security of the Rails Pay platform and CDE infrastructure	PCI compliance of their own systems, applications, and staff
Tokenisation and cardholder data minimisation	Implementing the correct integration method to minimise their scope
Encryption of cardholder data at rest and in transit	Not logging, storing, or caching cardholder data on their systems
Rails Pay incident response and breach notification	Reporting suspected compromises of their own systems to Rails Cloud
Maintaining Rails Pay SAQ and AOC documentation	Completing their own applicable SAQ annually
Amex SafeKey 2.0 platform implementation	Enabling SafeKey on their checkout flow and testing implementation

9. Contact and Documentation Requests

Enterprise customers, payment partners, and regulatory bodies may request the following documentation from Rails Pay's compliance team:

- Current SAQ (once completed Q2 2026) — available under NDA
- AOC (once issued Q1 2027) — available on request
- ASV scan summaries — available to direct enterprise integrators
- Penetration test summaries — available under NDA to qualifying partners
- DSOP alignment documentation for Amex partnership purposes

Query	Contact	Response Time
PCI compliance queries	compliance@railscloud.co	2 business days
AOC / SAQ document requests	compliance@railscloud.co	3 business days
Merchant PCI guidance	support@railscloud.co	1 business day
Amex / Nedbank partnership	enterprise@railscloud.co	1 business day
Security incident (payment)	security@railscloud.co	4 hours (24/7)