CardNest LLC

Customer Terms and Agreement

Table of Content

Introduction

These **Customer Terms and Agreement** (“Agreement”) govern the use of services provided by **CardNest LLC** (“CardNest,” “we,” “us,” or “our”), a fraud detection and prevention technology company utilizing advanced artificial intelligence and machine learning to protect businesses from online card transaction fraud.

By subscribing to or integrating with CardNest’s services, including but not limited to the **CardNest Security Scan**, **Card-At-Present™ engine**, and associated APIs (collectively, the “Services”), you (“Customer,” “You,” or “Client”) agree to be legally bound by this Agreement. If you do not agree to these Terms, you may not access or use the Services.

Scope of Services

CardNest provides a real-time, AI-driven fraud prevention platform that scans, detects, analyzes, and prevents suspicious and unauthorized card-not-present transactions. The platform is designed to be integrated with a business’s payment infrastructure via secure APIs.

Our services include:

- Real-time behavioral and credit/debit card analysis
- CardNest (CaP) Card at Present verification
- Cardholder validation and anomaly detection
- Predictive and Preventive fraud modeling and confidence scoring
- Real-time transaction evaluation and decisioning
- API integration for online merchants, remittance providers, and financial institutions

Use of Artificial Intelligence and Machine Learning

CardNest’s Services leverage its custom developed non-third-party AI/ML models that are trained using anonymized behavioral, transactional, and device metadata. Our system dynamically processes real-time data, including:

- Device and browser fingerprinting data
- Geolocation metadata
- Business or Merchant metadata/information during subscription
- Behavioral biometrics (e.g., hand movement, motion detections)
- Encrypted, tokenized data identifiers
- Tokenized transaction metadata
- Risk scoring inputs and outputs

The data processed is used solely for the purposes of fraud prevention and system optimization. Our models continuously improve in accuracy through secure, privacy-conscious learning methods.

Data Security and Compliance

No Cardholder Data Retention

CardNest does **not store, save, or archive** any cardholder data, including but not limited to:

- Magnetic Chip
- Magnetic Strip
- Magnetic Signature
- Hologram
- Card UV Logo
- Card Branded Logo
- Brand Customer Service details
- Card Symmetry
- Full card numbers (PAN)
- CVV/CVC codes
- Cardholder names
- Expiration dates

Real-Time Encryption Protocols

All scanned data is encrypted **in real-time using AES-256** bit encryption—the highest level of encryption accepted under the **Payment Card Industry Data Security Standard (PCI DSS)**.

Client-Side Decryption

Decryption of scanned transaction data occurs exclusively on the **Client's infrastructure** or authorized third-party platform preferred by the client. CardNest systems do **not perform decryption operations** nor retain any decrypted data.

Secure API Transmission

All data transferred to or from CardNest is transmitted using **TLS 1.2+** encryption protocols, with strict authentication measures and audit logging.

Client Responsibilities

The Client agrees to:

- Integrate CardNest APIs into its existing or new system following our documentation and best practices.
- Ensure compliance with applicable data protection and cardholder information laws (e.g., PCI DSS, GDPR, CCPA).
- Obtain any necessary end-user consents required for behavioral or transactional data processing.
- Not use CardNest's Services for illegal activities or in violation of applicable law.

Data Ownership and Usage

CardNest does not claim ownership over any data submitted by the Client but retains a license to scan, detect, analyze, process, and prevent such data for the purposes of:

- Delivering and preventing fraud detection decisions
- Model training and system enhancement (in anonymized format)
- Aggregate reporting and analytics (non-identifiable metrics)

We do **not sell, share, or monetize** client or customer data.

Service Availability and Uptime

CardNest will make reasonable efforts to ensure **99.9% uptime** of its systems, excluding scheduled maintenance or force majeure events. In the event of unscheduled outages, we will provide prompt communication and resolution through our support team.

Confidentiality

All customers or clients using our services and solutions agree to maintain the confidentiality of non-public business, technical, and financial information disclosed in relation to the Services. Neither party may disclose confidential information without prior written consent, except as required by law.

Billing and Payment

Pricing Structure

CardNest offers flexible billing options based on usage or scanning volume, features, and integration level, including:

- Standard scan per transaction
- Premium subscription packages
- Enterprise custom pricing

Clients will be invoiced in accordance with the selected plan or agreement.

Payment Terms

Invoices are payable within **30 days** of issuance unless otherwise agreed upon. Late payments may be subject to service suspension or additional charges.

Intellectual Property

All technology, software, models, content, and documentation provided by CardNest are the exclusive property of CardNest LLC. The Client is granted a non-exclusive, non-transferable, revocable license to use the Services for internal business purposes only.

Term and Termination

This Agreement begins upon the Client's acceptance and remains in effect until terminated by either party with **30 days' written notice**.

CardNest may terminate access immediately if:

- The Client breaches this Agreement
- Illegal or abusive usage is detected
- Payment obligations are unmet after 30 days

Upon termination, API access will be revoked, and all non-anonymized data will be purged in accordance with our no-storage policy.

Limitation of Liability

To the fullest extent permitted by law, CardNest shall not be liable for indirect, incidental, special, or consequential damages, including lost revenue or data, arising from the use or inability to use the Services—even if advised of the possibility of such damages.

Total liability is limited to the monthly subscription amount paid by the Client on the subscription Services in the previous **two (2) months to CardNest**.

Modifications to Agreement

CardNest reserves the right to update this Agreement. Clients will be notified of material changes at least **30 days in advance** via email or dashboard notification. Continued use of the Services after the effective date constitutes acceptance of the revised terms.

Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the **Commonwealth of Virginia**, United States, without regard to its conflict of law principles.

Contact Information

For any questions, requests, or concerns regarding this Privacy Policy or your data, please contact:

CardNest LLC
Email: **support@cardnest.io**
Website: **https://cardnest.io**