BEST PRACTICES KIT

Paystand Security Fact Sheet

Enterprise-class data security, management controls and fraud prevention

Paystand is the fastest growing commercial payments platform, supporting over 250,000 businesses paying on the Paystand payment network. The Paystand approach to security is rooted in the unique nature of B2B payments and provides the most robust, comprehensive payment security available.

At every step in the payment process, Paystand employs embedded safe-guards and protocols to ensure that payment information is secure.

Paystand protects your business and your customers with industry leading controls and technology:

- **Bank-grade data security** ensures all data remains secure whether in flight during a transaction or at rest in our database.
- **Advanced management control**s allow you to effectively manage user activity and keep your data secure from unauthorized access.
- **Proven fraud prevention tools** protect your transactions across all payment types to minimize chargebacks and avoid transaction risks.

Paystand.com
800.708.6413
Sales@Paystand.com

BANK-GRADE DATA SECURITY

PCI DSS Level 1 Certified

- Paystand maintains the payment industry's most stringent level of certification
- Why important: Ensures all card data is protected according to the highest industry standards

Fund on File Tokenization

- Paystand replaces used tokenization to safeguard a card's primary account number by replacing it with a unique string of numbers.
- Why important: Vaults your customers' payment information in a secure environment, allowing you to authorize, charge and re-use a customer's payment method without accessing their private information directly

Database Encryption & Password Hashing

- Paystand encrypts data at rest and key data as it is being processed with secure AES-256 encryption. Paystand also hashes all user passwords to an unreadable string of characters in the database.
- Why important: Ensures sensitive data and passwords are secure when being passed from users and when stored in our database.

ADVANCED MANAGEMENT CONTROLS

Role-Level Access

- Company admins can assign each user to a specific role with customized permissions and level of access. A complete audit trail with timestamps tracks all user activity on the Paystand platform.
- Why important: Allows admins to control and limit the ability of any corporate user to access customer and transaction information and use specific Paystand features. Also provides admins with full visibility into corporate user activity by login and user action.

Two-Factor Authentication

- When enabled, requires users to enter their password and a unique single-use code to access the Paystand platform.
- Why important: Protects each corporate user's account with a powerful level of additional security.

Payment Assurety

- Through Paystand's blockchain-based payment authentication process, each transaction automatically creates a digitized record trail that is secure, certified and fully auditable.
- Why important: Provides a verifiable receipt that your customers can access and print at any time to provide immutable proof of the transaction and related details.

PROVEN FRAUD PREVENTION

Credit Card Transaction Monitoring

- Advanced machine learning and transaction based scoring models analyze each transaction for potential fraud.
- Why important: Continuously monitors card transactions to detect and identify potential fraudulent activity and effectively reduce chargeback rates.

Paystand Smart Lockbox

- Paper checks are scanned and converted to electronic Check 21 format, allowing for automated data entry, remittance matching and reconciling deposits with your system of record.
- Why important: Increases deposit speed and reconciliation accuracy to significantly improve control and transparency, reducing potential for fraudulent check processing.

Paystand Zero Card for Corporate Expenses

- Advanced machine learning, ongoing rule analysis and 24/7/365 risk assessments continuously adapt to evolving fraud patterns.
- Why important: Ensures new and emerging fraud vectors are effectively identified through flexible and responsive fraud detection.