BEST PRACTICES KIT

Paystand Security Fact Sheet

Enterprise-Class Payment Processing, Security, Performance, and Compliance

Paystand is the fastest growing commercial payments platform, supporting over 140,000 businesses paying on the Paystand payment network.

Security is a key consideration in all that we do. No business can afford to overlook the need for protection against fraudulent activity and other abuse. That's why maintaining tight security using both traditional tools and advanced proprietary technology is a key part of Paystand's offering.

Advanced Fraud Protection

Paystand is a PCI Level-1 certified payment processor. This is the most stringent level of certification available in the payments industry. To accomplish this, we use best-in-class security tools and practices to maintain a high level of security.

Payment security is crucial for every merchant that stores, processes or transmits cardholder data. The PCI Data Security Standards help protect the safety of that data.

Paystand.com
800.708.6413
Sales@Paystand.com

Unlike other payment solutions, Paystand works closely with clients to prevent fraudulent payments which can lead to chargebacks and harm credit rating.

Paystand handles all the complexity involved with payment processing: PCI compliance, AML Laws, MTL Rules, Fraud Monitoring, Bank KYC Underwriting requirements, 1099K's - so you can sleep knowing your money is safe.

Fund on File Tokenization

Paystand uses tokenization to vault your customers' payment information in a secure environment. Tokenization is a process of replacing sensitive data with non-sensitive data. It is used to safeguard your card's primary account number (PAN) by replacing it with a unique string of numbers.

With a Fund on File token, users can securely authorize, charge, and re-use a customers' payment method without accessing their private information directly.

HTTPS Secure Connections

Paystand forces HTTPS for all services using TLS (SSL), including our public website and the Paystand Dashboard.

Database Encryption at Rest

Paystand's data is encrypted at rest with AES-256 at the database level. It uses an algorithm to transform data stored in a database into "cipher text" that is incomprehensible without first being decrypted.

Paystand encrypts key data as it is being processed. None of Paystand's internal servers are able to obtain plaintext customer information. Paystand's infrastructure for storing, decrypting, and transmitting customer information runs in separate hosting infrastructure and doesn't share any credentials with Paystand's primary services (API, website, etc.).

Hashed Passwords

Paystand hashes all user passwords, which means we convert passwords into unreadable strings of characters that are designed to be impossible to convert back, known as hashes.

Role-Level Access

Customers can assign each user on the account a specific role with permissions to only see and use the features related to their own duties. There is a complete audit trail that tracks activity by the user login and adds a timestamp for each action.

Two-Factor Authentication

Paystand offers two-step authentication that protects your account with an additional level of security. When you log in from a new device, we'll ask for both your password and a unique code.

Application-Only Access

The Paystand platform is divided into layers that separate your data from the software itself. Paystand users can only access the application features, and not the underlying database.

DDoS Resiliency

Paystand engineers have built in additional layers of resilience to prevent high volume attacks from taking down the paystand website.

Payment Assurety

Payment Assurety is the blockchain based payment authentication process unique to Paystand. Assurety automatically creates a digitized record trail that is secure, certified, and fully auditable. Every transaction over the Paystand Bank Network is recorded on a private blockchain and is accompanied by a verifiable receipt that your payers can access and print at any time.

Secure, Powerful APIs

You can have access to our full suite of OAuth secured, RESTful APIs, for whatever solution you need.