

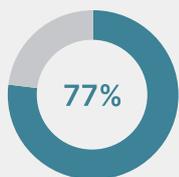
JAGGAER Pay AP Payments as Service Security Framework

Security, Quality, and Integrity are
Core to Our Culture and Services

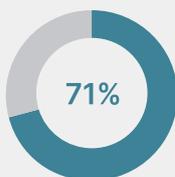


B2B Payments fraud is on the rise. Don't let your company fall victim by proactively upgrading your fraud prevention plan.

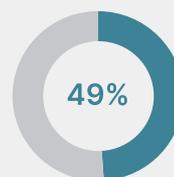
Most businesses are planning to invest in fraud prevention¹:



Desire to reduce payments fraud



Plan to implement new digital solutions to prevent fraud



Say finding a better digital solution for fraud prevention is their primary fraud prevention plan

¹ The Hidden Costs of B2B Payments Fraud, PYMNTS.com

Ensure your payments provider is equipped to mitigate fraud with bank-level security offerings:

JAGGAER Pay Features	JAGGAER Pay Capabilities
<p>Security against unauthorized access</p>	<ul style="list-style-type: none"> Enforcing a strong password policy Applying 2-Factor Authentication Sending login data over a secure channel — HTTPS required Single Sign On (SSO) with Multi-Factor Authorization (MFA) required for privileged data access Email mailboxes are encrypted and have advanced malware and phishing detection Enforcing separation of duties with role-based access that lets you control who can enter, approve, and pay bills JAGGAER Pay Portal automatically keeps a record of all AP activity with a timestamped audit trail of your payments and remittance details for each transaction

JAGGAER Pay Features	JAGGAER Pay Capabilities
Physical Security	<ul style="list-style-type: none"> All employees undergo background checks and data security and privacy training The platform is hosted within AWS Secure Cloud Ser4vices and relies on Amazon's implementation and adherence to their own physical security policies and practices. Data is housed in Amazon Aurora, powered by AWS
Risk & Compliance	<ul style="list-style-type: none"> Partnered with DYOPATH, one of the most trusted service-centric security & compliance providers in the world Annual SOC 1 and SOC 2 Type 1 & 2 Audits by a leading national CPA Firm Adopted an Anti-Money Laundering (AML)/Office of Foreign Assets Control (OFAC) Program, which is designed to prevent the Finexio Service from being used for purposes of money laundering, terrorist financing, violating or subverting OFAC sanctions, or for other illegal purposes Perform Know Your Customer ("KYC") to ensure accuracy and legitimacy of payment accounts Mitigate fraud and reduces risk through Bank Account Validation Services (AVS) to ensure money is moving safely and securely from the buyer to supplier
Payment Security	<ul style="list-style-type: none"> Reduce risk of check theft by paying vendors by virtual card or other digital payment methods Positive Pay is applied to reduce the risk of check fraud; the bank matches the check issued with the check presented for payment Keep your bank account information private from vendors by making digital payments through the JAGGAER Pay Portal
Network Security	<ul style="list-style-type: none"> Uses Amazon Web Services & firewall for intrusion detection, prevention of unauthorized electronic access to our servers
Data Security	<ul style="list-style-type: none"> Data center security is powered by AWS, and has certifications which include ISO 27001, SOC 1 & SOC 2/SSAE 16/ISAE 3402, PC1 Level 1, FISMA Moderate & Sarbanes-Oxley (SOX) NOC/SOC Network & Security Event Monitoring & Response systems are implemented for 24/7 monitoring, incident response, and incident management Continuity and regulatory backups are maintained by leveraging AWS RDS (Relational Database Security) Annual Disaster Recovery Plan tests to ensure rapid recovery to be proactive against any possible service disruption

MEA

+9714 360 1300
info-mena@jaggaer.com

APAC

+61 (2) 8072 0644
apac_sales@jaggaer.com

Americas

+1 919 659 2600
sales@jaggaer.com

Europe

+43 1 80 490 80
dach_sales@jaggaer.com