

rillion

The Accounts Payable Fraud Prevention Playbook



Table of Contents

1. Introduction
2. Types of Fraud in Accounts Payable Payments
3. Case Studies of AP Payments Fraud
4. Cyber Fraud is Increasing
5. Common Red Flags for AP Payments Fraud
6. Best Practices for Preventing AP Payments Fraud
7. Enhance Security & Control through Virtual Card
8. Reduce AP Payment Fraud by Moving to Electronic Payments
9. Technology Solutions for AP Payments Fraud Prevention
10. Focusing on Accounts Payable Payment Data to Fight Fraud
11. Best Practices
12. What Change Will You Implement By the End of Next Quarter to Fight
13. AP Payments Fraud?
14. Cyber Security Checklist
15. About Rillion

Introduction

Preventing fraud in accounts payable payments is crucial for any organization. Not only does it protect the company's finances, but it also helps maintain the integrity of the organization's reputation. Without proactive fraud prevention, actions by unknown or bad actors can cause legal repercussions. Fraud in accounts payable can take many forms, from invoicing scams to check and wire transfer fraud.

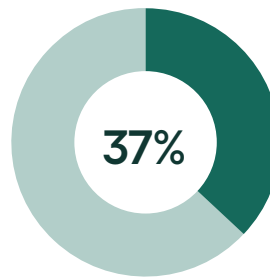
Here, we outline types of fraud that can occur in accounts payable, case studies involving the most common types of AP fraud, common red flags for fraud, the best practices, and technology solutions for preventing AP fraud. Ultimately, we close by describing which technology solutions are best to address AP payments fraud and how to make sure your chosen vendor has the right tools to help.

Types of Fraud in Accounts Payable Payments

Before looking at the different types of payment fraud, it is sobering to consider the prevalence of payments fraud across large and medium size businesses. In 2022:

-  **78%** of organizations experienced an attempt and/or actual payments fraud ⁽¹⁾
-  **71%** of organizations were targeted by Business Email Compromise (BEC) ⁽¹⁾
-  **59%** of organizations reported that their AP department was targeted by email phishing scams ⁽¹⁾

Invoice fraud: This type of fraud occurs when a criminal submits false or inflated invoices for payment. They may impersonate a legitimate vendor or create a fake vendor account to carry out the scam.



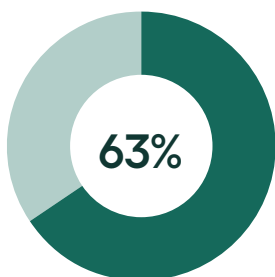
37% of businesses have no means to prevent an invoice scam. ⁽²⁾

There are several types of fraud that can occur in accounts payable payments. Payments fraud, most predominantly, includes:

Check fraud: Criminals can carry out check fraud by altering the payee's name, the amount of the check, or by creating counterfeit checks. They often use stolen checks, with the account information right at the bottom, to make unauthorized payments.

Wire transfer fraud: A criminal impersonates a legitimate vendor or employee and convinces an employee to wire funds to a fake vendor or a legitimate vendor's account that has been taken over by a fraudster. This type of fraud is appealing to scammers because the fraudulent result is untraceable after a short time.

Often wire transactions are completed and nearly impossible to retract after 72 hours. ⁽³⁾



63% of organizations were prey to check fraud in 2022. ⁽¹⁾

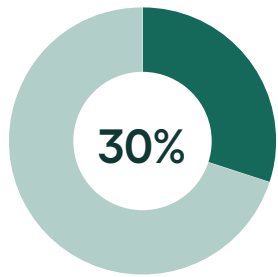


1. <https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud> AND <https://www.pymnts.com/tracker/b2b-payments-fraud-prevention-automation/digital-transformation/innovation>

2. <http://highradius.com/resources/Blog/best-practices-to-prevent-invoice-scams>

3. <https://www.forbes.com/sites/forbesbusinesscouncil/2022/08/30/wire-fraud-is-an-epidemic-take-these-threesteps-to-protect-your-company-from-cybercriminals>

ACH fraud: Automated Clearing House (ACH) fraud occurs when a criminal initiates an unauthorized electronic transfer of funds, such as direct deposit or electronic check payment from a company's account to their own account without authorization. Criminals may use stolen or fake bank account information to initiate fraudulent ACH transactions.



ACH fraud is the most common type of fraud. The share of fraud activity via ACH was 30% in 2022. ⁽⁴⁾

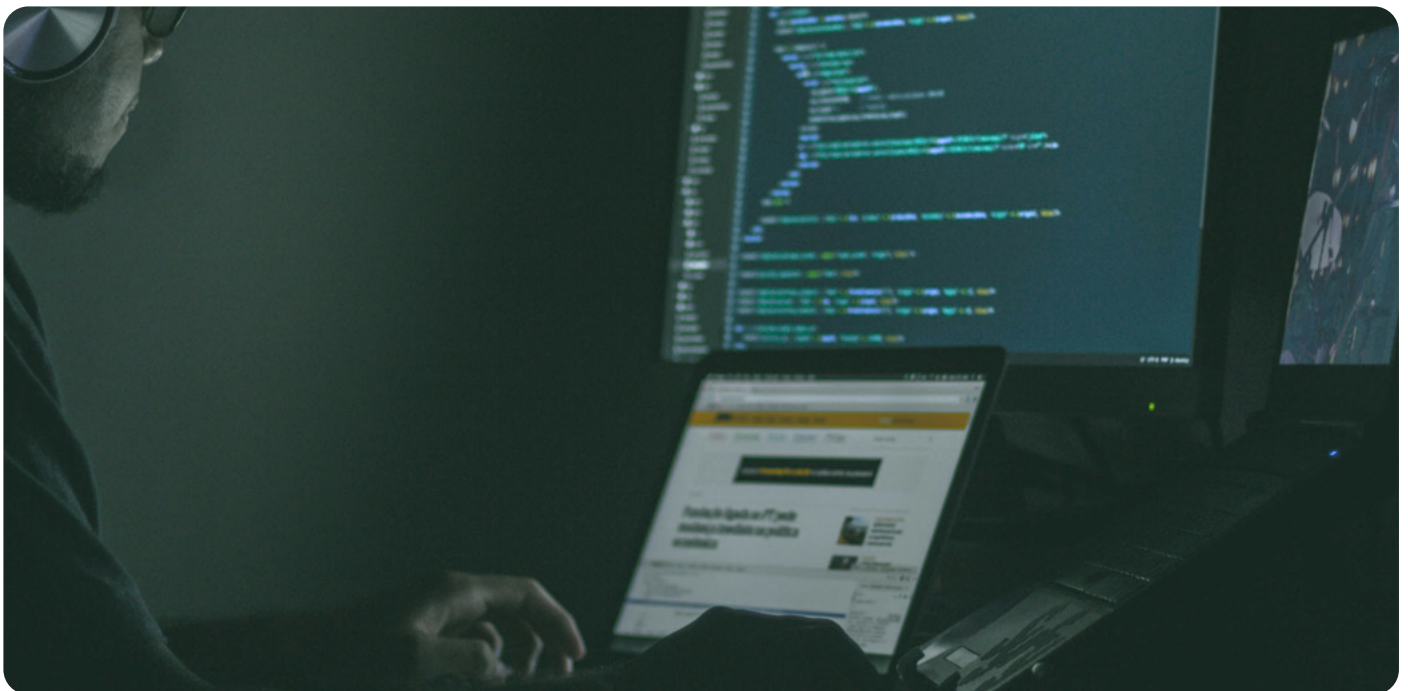
Speare Phishing fraud ⁽⁵⁾: When an email or other electronic communication is compromised to target an individual or organization impersonating a trustworthy source. The request in the communication seems legitimate and trustworthy but is, in fact, a scam to defraud the organization of resources, especially monetary resources. Often, this involves a combination of cloning a trustworthy source and installing malicious software on the target's devices. Email is most often used ⁽⁶⁾ to make this request or demand.

Otherwise known as Business Email Compromise (BEC), an impersonator can mimic a coworker or superiors in the requesting email. This is very hard to detect and looks very legitimate. BEC is a very efficient and effective way to put pressure on an unsuspecting employee ⁽⁷⁾ while delivering the very tools (malicious links and attachments in the email) to carry out the scam. It starts when an employee opens the email, which discreetly adds malicious software to their computer. Then when the employee complies with the request, the fraudster is given the basic information needed to use the malicious software without the employee knowing. This can cause significant payment delays, investigations, and additional KYC/KYB requirements.



90%

of data breaches occur due to phishing ⁽⁸⁾, primarily involving Business Email Compromise



4. <https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud>

5. <https://usa.kaspersky.com/resource-center/definitions/spear-phishing>

6. <https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishingemail-to-an-unexpected-victim.html>

7. <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise>

8. <https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/>

Case Studies of AP Payments Fraud

Over the last few years, authorities have become increasingly vigilant with accounts payable fraud. It does not matter if it is a financial decision maker or accounts payable clerk, fraud opportunities are available up and down the roster of AP staff. Some memorable incidents include:



Yale employee embezzles \$40M, forced to return Mercedes

A recent case of wire fraud, among other misappropriations, found that a lead administrator and director of finance and administration for the Department of Emergency Medicine at Yale University in New Haven, Conn, was falsifying documents and arranging for fraudulent purchases⁽⁹⁾ resulting in a lavish lifestyle for herself but a loss of \$40M for Yale.

According to the New York Times, the fraudster, now convict, and former Yale employee “... admitted that she had submitted thousands of purchase orders for computer devices and tablets that included Microsoft Surface Pros and iPads under the pretense that they were for medical studies, according to the F.B.I.”

The perpetrator received 9 years in prison and agreed to pay back over \$40M in losses to Yale.



Accounts payable clerk stashes \$300,000 from gift shop

According to Justice.gov,⁽¹⁰⁾ over a two-year period, this not so creative fraudster shorted vendor payments, transferring the difference

into his own accounts and altering records to cover up his crimes. In some cases, he didn't pay the vendors at all and transferred the funds to an account of a friend.

The small business he stole from was a gift shop, an enterprise not known for being cash rich. After serving his time for 10 counts of wire fraud, he was ordered to pay \$302,995 in restitution and serve the next few years in a combination of prison, a half-way house, and lengthy probation.



Facebook and Google fall for fraud to the tune of over

\$100M in losses Payments Journal⁽¹¹⁾ reported in 2019 that both Facebook and Google were bilked out of over \$100M by a single individual who is now facing over 30 years behind bars.

The fraudster's ability to impersonate a known vendor highlighted how even the biggest tech giants can fall for fraud based on familiarity and complacency. It also highlights how three-way matching is no longer enough to deter crimes like this.

In this case, both tech companies did business with the same vendor. Both companies failed to notice discrepancies in billing. And both companies failed to verify that the criminal was actually a legitimate vendor.

9. <https://www.nytimes.com/2022/04/01/nyregion/yale-administrator-guilty-jamie-petrone.html>

10. <https://www.justice.gov/usao-ri/pr/accounts-payable-clerk-sentenced-fraud>

11. <https://www.paymentsjournal.com/google-facebook-100-million-accounts-payable-fraud/>

Cyber Fraud is Increasing



Increase in corporate cyber attacks last year ⁽¹²⁾

\$1.85 M

Recovering from a ransomware attack cost businesses \$1.85 million on average in 2021 ⁽¹³⁾

\$20 BN

Ransomware cost the world \$20 billion in 2021. That number is expected to rise to \$265 billion by 2031 ⁽¹³⁾



Of all businesses and organizations were hit by ransomware in 2021 ⁽¹³⁾

Common Red Flags for AP Payments Fraud

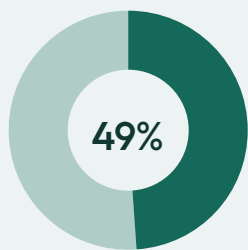
Any strange payment activity should be carefully reviewed and investigated. There are several common red flags that can show fraudulent activity in accounts payable payments, including

Unusual payment requests: This could include requests for wire transfers to unfamiliar vendors or payments in unusual amounts. This can also include the payment to be made to a personal account.

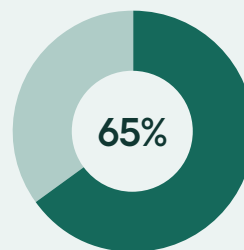
Unfamiliar vendors: This could include vendors that have not been used before and are not in the company's regular network of suppliers. Suppliers should be thoroughly vetted and regularly checked before making payments. Those that have recently changed their contact information or banking details are especially susceptible to being compromised.

Missing documentation: This could include invoices or purchase orders that lack important information or have been altered.

Pressure to expedite payment: Fraudsters often try to rush the payment process to avoid detection. They apply pressure to make a payment quickly, without proper documentation or verification, which can be a sign of fraudulent activity.



Say finding a better solution for fraud prevention is their primary fraud prevention plan ⁽¹⁴⁾



Of organization AP departments were victims of payments fraud ⁽¹⁴⁾

- 78% of companies with more than \$1B in revenue
- 60% of companies with less than \$1B in revenue

12. <https://www.cybersecurityintelligence.com/blog/corporate-cyber-attacks-up-50-last-year-6069.html>

13. <https://www.cloudwards.net/ransomware-statistics/>

14. <https://www.pymnts.com/tracker/b2b-payments-fraud-prevention-automation-digital-transformation-innovation/> AND <https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud>

Best Practices for Preventing AP Payments Fraud

To prevent fraud in accounts payable payments, companies should implement the following best practices:

Move to Electronic payments: Check payments have never been a safe option. Electronic payments such as virtual cards can help reduce the risk of check fraud and can help detect fraudulent activity more quickly.

Implementing a strong internal controls system: This includes procedures for verifying vendor information, reviewing and approving invoices, purchase orders, payments, and other documentation related to accounts payable as well as reconciling accounts.

Regularly reviewing and updating vendor information: Keeping accurate and up-to-date information, such as contact information, banking details, and other important information on vendors to help detect any potential fraudulent activity.

Creating a system for reporting suspicious activity: This can include setting up a hotline or email address for employees to report potential fraud. Employees should be trained

on how to recognize and report suspicious activity, and there should be a simple process in place for reporting and investigating potential fraud.

Training employees on how to identify and prevent fraud: This can include educating employees on the common red flags for fraud and providing them with the tools and resources they need to identify and prevent fraud.



Per AFP, only 9% of attempted fraud was on a virtual card ⁽¹⁵⁾ vs 63% on checks



Enhance Security & Control through Virtual Card

Virtual Cards add control to the payables process with enhanced security features and adaptable controls that mitigate the risks of fraud and misuse. Here are the key security and control enhancements:

- **A single-use**, unique 16-digit account number is assigned to each payment.
- **Cards are locked** into a specific amount of available credit for a limited time.
- **No bank information** is required for set up or payment transmission.
- **Visibility is increased** and internal control is centralized through a single department.
- **Use is authorized** only after all proper approvals have been obtained.
- **The payment reconciliation** period is shortened and transaction risk is reduced.



12. <https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud>

Reduce AP Payment Fraud by Moving to Electronic Payments

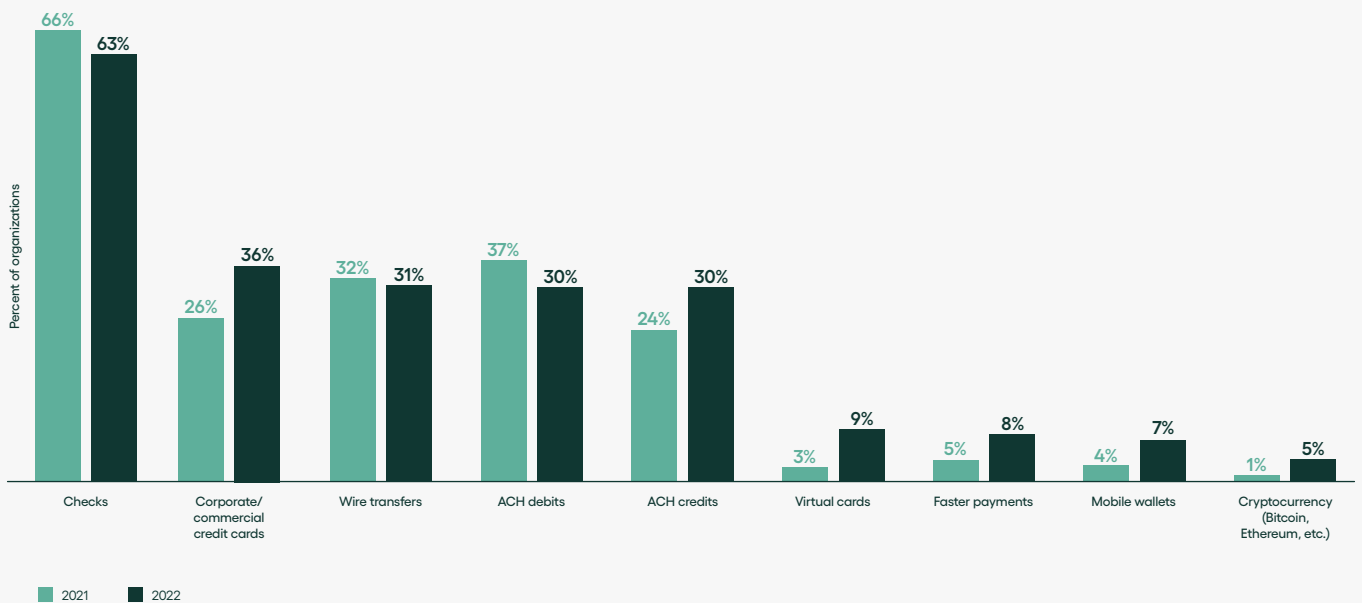
Virtual Cards add control to the payables process with enhanced security features and adaptable controls that mitigate the risks of fraud and misuse. Here are the key security and control enhancements:

- **A single-use**, unique 16-digit account number is assigned to each payment.
- **Cards are locked** into a specific amount of available credit for a limited time.
- **No bank information** is required for set up or payment transmission.
- **Visibility is increased** and internal control is centralized through a single department.
- **Use is authorized** only after all proper approvals have been obtained.
- **The payment reconciliation** period is shortened and transaction risk is reduced.



Check fraud is prevalent in **63%** of organizations experiencing fraud.

Checks are **7X** more likely to be involved in fraud than virtual cards.



Source: 2023 AFP Payments Fraud and Control Survey, Percent of surveyed organizations where payment methods were subject to attempted/actual payments fraud.

Data should be cleaned and enriched to ensure accuracy and completeness. This involves removing duplicates and inaccuracies, adding missing information, and using data analytics to identify patterns and trends. Payment data validation and error handling should also be implemented to prevent data issues that would delay payments. Data enrichment can improve supplier information, leading to better electronic payment conversion and decreased fraud risk.

AML Compliance: Transaction Monitoring can efficiently detect, investigate and report suspected money laundering activity or suspicious activity, to comply with current and future regulations and guidelines. Data enrichment can improve supplier information, leading to better electronic payment conversion and decreased fraud risk.

Know Your Customer (KYC)/Know Your Business (KYB) processes should be used by organizations to verify the identity of each customer or business to ensure they are not doing business with bad actors.

These are a specific set of processes that require deep dives into a company's management, industry, payment volumes, product, and services rendered.

KYB is an offshoot of KYC that more specifically refers to validating a business's existence, validating that it is in good standing, and trustworthy.



AP PaaS providers, like Finexio, can do this and so much more. They can help improve the adoption of electronic payments, verify and enhance the relationship with suppliers and other partners, decrease fraud, cut costs, and enhance companies' visibility into their payments processes.



Technology Solutions for AP Payments Fraud Prevention

Besides implementing best practices, companies can also use holistic technology and software solutions to prevent fraud in accounts payable payments, including:

Implementing AP Payments as a Service can help improve the adoption of electronic payments, verify and enhance the relationship with suppliers and other partners, decrease fraud, cut costs, and enhance the visibility companies have into their payments processes.

Automated invoice processing: Automating the invoice process can help quickly identify, flag, detect, and prevent fraudulent activity like fake invoices by providing real-time visibility into invoice data and automating the approval process.

Positive Pay systems⁽¹⁶⁾: Positive pay systems can help prevent check fraud by matching the check being presented for payment against a list of checks the company has authorized.

Fraud detection software⁽¹⁷⁾: Fraud detection software can help organizations quickly identify suspicious activity by analyzing transaction data from multiple sources such as vendor information, invoice data, and payment history to identify patterns that may indicate fraud.

According to the Faster Payments Council survey, 50% had experienced invoice fraud and 64% had experienced vendor impersonation fraud⁽¹⁸⁾

16. <https://www.investopedia.com/terms/p/positive-pay.asp>

17. <https://www.gartner.com/reviews/market/online-fraud-detection>

18. <https://fasterpaymentscouncil.org/blog/8621/2021-Faster-Payments-Fraud-Survey-and-Report>

Focusing on Accounts Payable Payment Data to Fight Fraud

Of the technology solutions for fraud prevention in AP payments that we listed above, the most effective solution is using an AP Payments as a Service (PaaS) provider but with additional features and services. Using a PaaS provider will encompass the best aspects of the technology solutions available before, during, and after fraud detection.

PaaS providers, like Finexio, leverage payment data management and security to thwart fraud while improving other areas of the payments process. The right PaaS provider will couple technology solutions

with human-enabled outreach to maximize opportunities and solve problems. These three fraud-fighting characteristics of great PaaS providers can help you fight fraud by securely collecting, validating, encrypting and storing account information, cleaning and enriching data, and ensuring that your payments are safe and secure.



Best Practices

When evaluating a PaaS provider, be sure to ask about their technology and services using the following best practices as your guide:

Account information should be securely collected. When collecting customer account information, it is important to use secure methods such as SSL or TLS encryption to protect the data in transit and at rest.

Billing information should be checked and updated to ensure supplier banking data is protected and secured safely. Ensuring that provided payment information is complete and valid is important to reducing risk, and preventing late or dropped payments.

Bank Account Validation (AVS) will prevent unauthorized changes to your account and to your vendor's account information. Your PaaS provider should validate bank accounts (ensuring routing number and account structure via a NACHA approved service provider) and monitor when bank account information is changed to verify accuracy of information. This checkpoint ensures that money safely and securely flows to and from where it is supposed to go.

OFAC Sanction Screening — Sanctions Screening is a must for helping businesses detect, respond and eliminate inherent and residual money laundering. OFAC (The Office of Foreign Assets Control) Sanctions lists and AML (Anti-Money-Laundering) compliance checking should be implemented on all accounts. This also helps identify and eliminate terrorist financing and fraud-related risks. Not only will this prevent fraud but it will also reduce liability for businesses.

The data should also be encrypted and stored in secure data centers, and multi-factor authentication (MFA) and single sign-on (SSO) should be used for secure access. To further ensure data security, it is important to monitor access, reevaluate user and administrator access, use advanced email security, and protect against phishing.


What Change Will You Implement By the End of Next Quarter to Fight AP Payments Fraud?

Preventing fraud in accounts payable

is crucial for any organization. Safe payment systems can be put in place with processes and technology available today. By understanding the different types of fraud that can occur, the common red flags for fraud, and the best practices for preventing it, organizations can take steps to protect themselves from financial loss and reputational damage. Technology solutions can provide added protection against fraud.

Organizations need to stay vigilant and continuously review and update their payments systems and processes to be ready and able to face the fraud threatening their accounts payable payments.

Instead of building it yourself or cobbling together an incomplete solution, use the services of an AP Payments as a Service provider, like Finexio. This will give you access to the fraud-fighting tools and talent you need. Finexio can help you improve the adoption of electronic payments, verify and enhance your relationship with suppliers and other partners, decrease fraud, cut costs, and provide enhanced visibility into your payments processes.



Avoid the pain of building your own accounts payable payments fraud-fighting machine. **Book a Demonstration with Rillion.**

Cyber Security Checklist

When considering an AP Payments as a Service provider, make sure that they adhere to the following industry standard best practices in payment data management and security protocols:

Audit Current Systems and Suitability of the Design of Controls Security

- Recovery
- Incident Management
- Designing, Testing & Deploying
- Risk Assessment
- Integrity & Ethical Values

Network Operations Center (NOC) and Security Operations Center (SOC) Measurement and Success Metrics

- Centralized Logging
- Vulnerability Scanning
- Operational and Security Event Monitoring
- Incident Response
- Incident Management
- 24x7 Monitoring

Corporate Identity Access and Management

- Centrally managed user provisioning
- Multi-Factor Authentication (MFA) required for user authentication
- Role-based permissions for granular access to systems and data

- Conditional Access policies define access rules to determine how and when users can authenticate
- Sign-in logs — Validate/identify suspicious user activity

Data Center Security

- ISO 27001 Certification
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (previously SAS 70 Type II) Certifications
- FISMA Moderate Certification
- Sarbanes-Oxley (SOX)
- Physical access control with security badges or biometrical security (security personnel on site 24/7)
- Security cameras monitoring the data center locations 24/7
- Fully redundant and maintainable power supply with backup power supply to provide 24/7 continuous uninterrupted power
- Monitor and perform preventative maintenance of electrical and mechanical equipment

Email Security

- Email mailboxes are stored in encrypted format
- Two-factor authentication required for email

- Attachment scanning to detect viruses or malware
- Advanced malware, phishing, and anomaly detection and continuous education
- Domain-based Message Authentication, Reporting and
- Conformance (DMARC), Sender Policy Framework (SPF), and mail signing with DomainKeys Identified Mail (DKIM)

Network Security

- A firewall, such as Amazon Web Application Firewall (WAF) is used to protect the system by blocking unwanted traffic to or from the system
- Military Grade Encryption: RSA 2048 bits keys - Supports TLS 1.2 or 1.3, SHA-256, and HTTP Strict Transport Security (HSTS)
- Routine monitoring of firewall and IDS logs and configurations
- Routine review of user access to the production environment
- Tenable.io Vulnerability Scanning — Provides comprehensive and accurate vulnerability scanning, to proactively identify and remediate potential areas of attack and reduce risk
- Security Information and Event Management (SIEM) for security event logging, orchestration, and response along with Intrusion Detection and Prevention

Database Security

- Data is housed securely, such as in Amazon Aurora, backed by a distributed, fault tolerant, self-healing storage system
- Data at rest and data backups are encrypted with the most robust Advanced Encryption Standard industry standard variant, AES-256
- Data in transit is encrypted over a secure channel

- Documented business continuity plan and disaster recovery plan, which is tested annually

Application Vulnerability Scanning and Remediation

- Automated scanning to continuously detect and report on the vulnerabilities found within the application
- Software library scanning to identify issues with 3rd party libraries/code
- Container scanning to identify vulnerabilities at the OS level
- Dynamic Scanning to proactively detect and identify potential vulnerabilities in application workflow and implementations
- Remediation and validation of findings to ensure security risks are addressed and properly handled
- Internal and external penetration testing (pen testing)

Organizational Security

- Non-Disclosure Agreements
- Employee Background Checks
- Endpoint Security
- Annual Confidentiality and Security Awareness Training

Platform Security

- Continuous Integration/Continuous Deployment
- Single Sign-On (SSO) with Multi-Factor Authentication (MFA)
- HTTPS Required
- Admin roles reviewed and updated on a regular basis
- User roles defined with the principles of least privilege access

About Rillion

Rillion is a leader in AP automation and B2B payment solutions, helping businesses streamline financial operations with secure and efficient payment processes. With over 30 years of experience, Rillion empowers finance teams by automating invoice capture, 3-way PO matching, AI-driven workflows, and secure payment processing. Trusted by over 3,000 companies worldwide, Rillion integrates seamlessly with ERP systems, reducing manual work, enhancing compliance, and mitigating payment risks. Our intelligent automation platform ensures businesses gain control, visibility, and efficiency in their accounts payable and payment processes.

To learn more, visit www.rillion.com.



rillion