Deluxe Payment Exchange+

3 Key Steps to Help Ensure Payment Security

What to look for in your next payment platform

deluxe+
PAYMENTS & DATA

White Paper

79%

of organizations were targets of an attempted or actual payment fraud in 2024.[1]

As traditional paper check usage continues its downward trend, more organizations are looking to incorporate digital payment solutions into their business-to-business (B2B) offerings. But, while a shift to digital payments saves time and money, businesses also need to heighten their security measures to prevent fraud risk.

Paper check fraud makes up a significant portion of fraud attempts in the U.S. each year, with more than 60% of organizations reporting check fraud activity.[1] As check fraud continues to rise, companies are considering more secure digital payment alternatives. In 2024, 20% of organizations indicated that after a successful fraud attempt, they were unable to recover the funds lost due to the fraud.[1]

"Businesses, particularly larger businesses, find great value in solutions that help reduce check fraud risk. It's not just the hard dollar loss, but the reputational risk that comes along with fraud, and the time that the business has to invest to rectify a fraudulent payment," says Steve Buchberger, Executive Director of Payables Product Management at Deluxe. To meet the need for heightened security, it's important to select a payment provider that has the critical capabilities to best protect your organization from increased risk of fraud and security issues.

1 in 5 organizations indicated that after a successful fraud attempt, they were unable to recover the funds lost due to the fraud.[1]

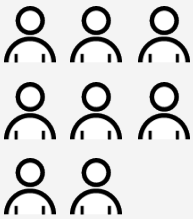
[1]2025 AFP Payments Fraud and Control Survey Report, April 2025.

Step 1:
Understand the physical risk of fraud

The average paper check is handled by up to eight people, creating increased opportunity for physical fraud, especially check alteration and counterfeiting. The chances of physical fraud also increase when these checks are left in unattended mailboxes where they can be easily stolen. Mailing sensitive information like account holder name, account number and routing number makes paper checks vulnerable to these fraud attempts. Part of the vulnerability of checks is mail interference. In 2024, AFP reported that 23% of organizations experienced check fraud due to mailbox thefts.[1]

By moving to an integrated payables platform, the number of people handling the payment is reduced to two people: the payer and the payee. The risk of physical check fraud is eliminated by using digital payment methods. In addition to helping reduce fraud risk, digital payments offer many benefits to organizations, such as low implementation costs, optimized cash flow and decreased payment processing time.

Paper check handling?



8 people on average

Digital payment handling?

2 people on average

Most common fraud risks for paper checks and their solutions:[2]

The Risk	The Solution
Alteration	Use high-security check stock with detection features (such as thermochromic ink, holograms and security fibers within the check itself) to indicate whether or not a physical check has been tampered with.
Counterfeiting	Positive Pay provides regular updates to the bank to identify legitimate payments from fraudulent claims.
Account Takeover	Use real-time verification measures and levels of account permissions to decrease the likelihood of account takeover.
Embezzlement	Employ a separation of account controls and permissions

[2]Internal Deluxe Payment Exchange+ data.

Step 2:
Secure your digital payments

While a shift to digital payments has increased payment efficiency and eliminated physical fraud, the use of technology still leaves opportunity for criminals to attempt fraudulent payments. Traditional paper checks and wire transfers are the two most common payments impacted by fraud activity: 63% of financial professionals reported fraud activity with paper checks and 30% with wire transfers in 2024.[1]

Selecting the right automated payables vendor is key to help ensure your payments are secure and efficient. Your payment provider should offer several capabilities to decrease the chance of fraud and protect your business in four main areas: account access, payment delivery and retrieval, payment deposit and overall platform security.

Account access:

- Account creation should take place within a secure platform with strong password and user information protection
- Require Multi-factor Authentication (MFA) for all users logging onto the platform to ensure secure access
- Set up a separation of account controls by account administrator to allow certain employees to create, sign and send payments
- Use solutions that require account verification whenever a new account is added into the payment platform

Payment delivery and retrieval:

- Payments should only be retrieved from an encrypted, secure platform and not from an email attachment
- Use a solution that provides a digital fingerprint that tracks all interactions with a payment (who issued, who approved, who received, when received, etc.) such as a cryptographic timestamp

- Use a system that allows the receiver of the payment to enter their own banking information and select their preferred method of payment
- Use a solution that eliminates the need to collect and store sensitive payment details such as Personally Identifiable Information (PII) from the payee organization and its employees
- Enhance security by choosing an option to void the digital payment within the vendor's online payment platform in real time

Payment deposit:

- Require Positive Pay files to be sent between financial institution and payment provider to prove legitimate transactions
- Implement a level of fraud protection for payers; consider a vendor with additional safeguarding options (i.e., to avoid counterfeit checks or forged signatures)

Overall platform security:

- Ensure your payment provider platform is compliant with privacy laws and regulations

Step 3:
Maintain strict compliance to changing regulations

A significant part of ensuring the success of your payment platform is to be secure and compliant with ever-changing state regulations and national privacy laws. Your platform's overall security depends on staying compliant.

Personally Identifiable Information (PII) such as name, account number and other banking information must be kept secure. By using encryption and account verification, the PII housed in your payment platform is far less susceptible to fraud.

A secure, compliant platform for your payments

Deluxe Payment Exchange+ (DPX+) provides comprehensive, end-to-end security measures to actively help eliminate the risk of fraud and security issues within its platform.

Deluxe Payment Exchange+ has all the critical key capabilities that your business needs to efficiently pay and get paid within a secure, compliant platform. With an industry-proven partner like Deluxe, security is a top priority. This integrated payables platform gives your business the speed and ease of digital payments, backed by the security expertise and support of a 110-year-old business technology partner.

By leveraging digital technology, Deluxe adds value from a delivery and cost standpoint, but also makes perpetuating fraud more difficult through its security measures. DPX+ maintains security compliance with AICPA SOC-2 certification, built-in PCI and NACHA regulation standards..

The critical security capabilities of Deluxe—real-time verification, positive pay, separation of account access controls and overall platform compliancy—significantly help reduce the risk of fraud in digital payments.

How prepared is your organization to migrate to a secure, automated payables solution?

Answer these questions to assess your readiness:

- ☐ Do you have Positive Pay set up with your existing payment rails? Consider adding this to your digital payment offerings as a best practice.
- ☐ Does your payment provider offer a real-time verification service for new and existing accounts?
- ☐ Can you apply a separation of controls within your payment platform to prevent risk of embezzlement or internal account takeover—especially with an ongoing remote working environment?
- ☐ Can you offer easy deposit options to your payee?
- ☐ How easily can an integrated payables solution merge into your current accounting processes and programs?
- ☐ How will adding digital options affect your compliancy process?

» Learn how to help increase the security of your digital payments

» Contact your Deluxe representative or visit **deluxe.com/dpxplus**

dlx