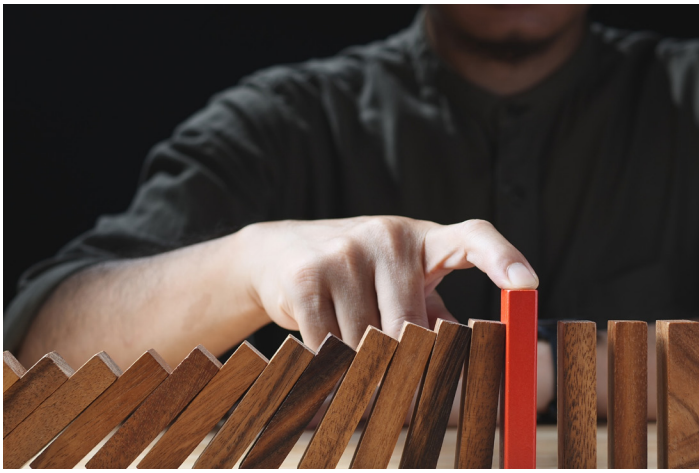
Treasury Payments Risk Management

Historically, risk management in payments focused primarily on ensuring accuracy and maintaining operational continuity. While these remain pertinent factors, organizations must also recognize that the landscape has evolved with new risks from the rise of digital transactions, increased cyber threats, and more complex global payments. A recent survey by the Association for Financial Professionals estimates that 65% of organizations were victims of payment fraud attacks or attempts last year and that almost half of those affected were unable to recoup lost funds. The scale of the problem is impossible to overlook, with the cost of ransomware attacks on businesses exceeding $1 billion for the first time in 2023. With new risks emerging at an unprecedented pace, companies must remain vigilant and adopt best practices for fraud prevention and detection.



The good news is that the past five years have seen a substantial surge in the advancement and adoption of technology to combat payment fraud, driven by rapid developments in artificial intelligence and machine learning. It is imperative for any modern payment strategy to incorporate these solutions as a primary means of risk mitigation. There are a variety of tools available, including:

- **Multi-Factor Authentication (MFA):** MFA can be implemented to require users to verify their identity through multiple means, such as passwords or biometrics when inputting or approving payments. Most treasury and finance systems already support multi-factor authentication. With applications such as Google Authenticator and Microsoft Authenticator freely available, MFA can provide a cost-effective way of immediately improving the security of payment processes.
- **Encryption and Digital Signatures:** encryption can protect sensitive financial information during transmission, safeguarding payment details (such as account numbers and transaction amounts) from interception and tampering by rendering the data indecipherable to unauthorized entities. Simultaneously, digital signatures provide a robust mechanism for verifying the authenticity and integrity of digital messages or documents, helping ensure that payment instructions and authorization requests are genuine and unaltered.
- **Fraud Detection Platforms:** advanced artificial intelligence and machine learning algorithms can analyze payment datasets to identify anomalous patterns and detect potentially fraudulent transactions in real time. For example, alerts can be automatically generated for any cross-border payment to a country that is not on the list of locations in which the firm typically operates or for a first-time transfer to a new account associated with an existing supplier.

- **Behavioural Analytics Software:** focus on user behavior patterns to identify anomalies and potential fraudulent activities. This technology relies on the understanding that individuals have unique digital fingerprints based on their typical actions, such as transaction history, login times, and device preferences. By continuously analyzing and learning from these patterns, behavioral analytics software establishes a baseline of normal behavior for each user. When unusual activities deviate from this baseline, the system raises alerts or flags potentially fraudulent transactions.
- **Validation of Beneficiary Information:** automated processes can cross-reference beneficiary information against trusted databases, flagging discrepancies or inconsistencies that may indicate fraudulent activity. Blockchain technology is increasingly employed for secure and tamper-resistant record-keeping, reducing the risk of unauthorized alterations to beneficiary data.

Organizations should complement the implementation of these technology solutions by:

- Fostering a culture of security awareness through regular employee training and encouraging prompt reporting of any suspicious activity.
- Implementing strict internal controls and periodic security audits and assessments to identify and address potential vulnerabilities and reduce the risk of internal fraud.
- Rationalizing banking partners to reduce payment file formats and transmission method variations.
- Strengthening bank and vendor relationships with thorough verification processes and ongoing due diligence to provide an additional layer of protection.

Investing time in implementing comprehensive fraud prevention and detection measures and encompassing both technological and non-technological strategies is essential for organizations, given the potentially significant costs associated with payment fraud. From a monetary perspective, the financial losses incurred through fraudulent activities can be substantial, impacting the bottom line and diverting resources. Additionally, the reputational damage resulting from payment fraud can be long-lasting, eroding trust among clients, partners, and stakeholders. By dedicating resources to robust fraud prevention measures, organizations safeguard themselves against financial losses and protect their reputation, fostering trust and stability in their operations.