5 essential tips to protect your organization from payment fraud

Unlock resiliency by fortifying your defenses

In today's complex financial environment, payment fraud is an inevitable challenge rather than a distant possibility. With sophisticated threats like business email compromise (BEC) and deep-fake technology on the rise, maintaining operational speed without compromising security is critical. How can you ensure your organization remains resilient?

1. Secure the entry point with vendor onboarding

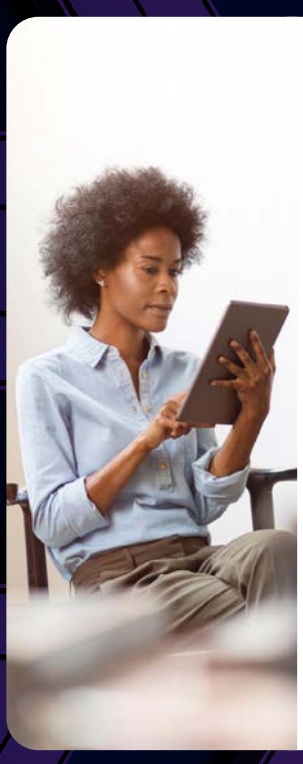
The challenge:
The most common entry point for fraud often lies in the initial setup of vendor data. If incorrect or fraudulent bank details are entered into your master file, every subsequent payment to that vendor is compromised. Fraudsters frequently target this vulnerability by impersonating suppliers and requesting changes to payment instructions.

How to overcome It:
- **Standardize the process:** Implement a strict, documented workflow for adding new vendors that requires multiple levels of approval.
- **Validate bank details:** Use "out-of-band" verification – such as calling a trusted contact at a verified number – before accepting any changes to payment instructions or bank account details.
- **Leverage validation services:** Utilize third-party tools to verify that the bank account owner matches the vendor name before the first payment is ever sent.

2. Automate oversight with anomaly detection

The challenge:
As transaction volumes grow, manual review becomes impossible. Fraudsters rely on this "noise" to hide illicit transactions. They may send payments that are slightly higher than usual or increase the frequency of payments to a compromised vendor, knowing that human reviewers might miss these subtle deviations.

How to overcome It:
- **Deploy AI-driven tools:** Move beyond static rules. Implement systems that use machine learning to understand "normal" payment behaviors for your organization.
- **Scan in real time:** Ensure your monitoring tools can flag irregularities such as unusual amounts, timing or beneficiaries, before the funds leave your account.
- **Investigate deviations**: Establish a clear protocol for halting and investigating any transaction flagged as an anomaly, regardless of the urgency.



3. Strengthen the human firewall through employee training

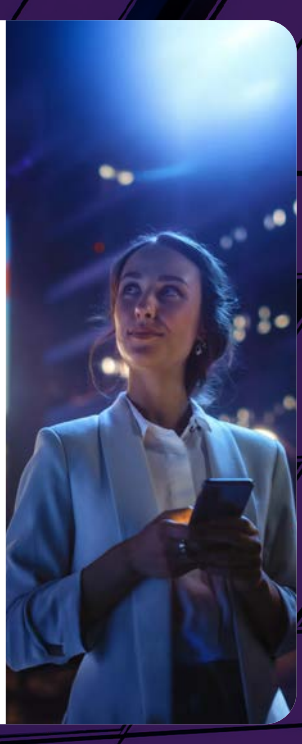
The challenge:
Your employees are both your greatest asset and your biggest potential vulnerability. Criminals exploit human psychology through urgency and authority, often impersonating C-suite executives to pressure staff into bypassing standard procedures. Without specialized training, employees may unknowingly authorize fraudulent transfers.

How to overcome It:
- **Conduct role-specific training:** Provide targeted education that addresses the specific threats relevant to treasury and AP roles, such as spotting the signs of BEC.
- **Empower verification:** Foster a culture where employees feel safe questioning urgent requests, even those appearing to come from senior leadership.
- **Test readiness:** Run regular, simulated phishing attacks to gauge employee awareness and identify areas where additional training is needed.

4. Lock down access using multi-factor authentication (MFA)

The challenge:
Compromised credentials remain a leading cause of unauthorized access to payment systems. Relying solely on passwords leaves your financial portals vulnerable to phishing attacks and credential stuffing. Once a fraudster gains access, they can manipulate payment files or approve fraudulent transactions with ease.

How to overcome It:
- **Mandate MFA everywhere:** Enforce multi-factor authentication for all users accessing bank portals, ERPs and treasury management systems.
- **Review access rights:** Regularly audit user permissions to ensure strict segregation of duties; no single individual should have the ability to initiate and approve a payment.
- **Monitor login activity:** Set up alerts for suspicious login attempts, such as access from unrecognized devices or foreign locations.



5. Future-proof your defense with regular security assessments

The challenge:
Fraud tactics evolve rapidly. A defense strategy that was effective two years ago may be obsolete today. Many organizations fail to update their protocols until after a breach has occurred, leaving gaps that criminals are eager to exploit.

How to overcome It:
- **Schedule annual reviews:** Conduct a comprehensive internal review of your end-to-end payment process at least once a year to identify new vulnerabilities.
- **Engage external experts:** Every two years, bring in third-party consultants to perform an objective assessment of your security posture.
- **Align with regulations:** Ensure your processes are ready for upcoming industry mandates, such as NACHA's fraud detection rules and SEPA's Verification of Payee requirements.

Building a fortress to protect your payments processes does not require sacrificing efficiency. By addressing these five critical areas, you can transform your fraud prevention strategy from reactive to proactive. A secure payment process is the foundation of a resilient, trustworthy and efficient treasury operation.

Contact FIS

Money at rest. Money in motion. Money at work.™

Our technology powers the global economy across the money lifecycle.

Money at rest
Unlock seamless integration and human-centric digital experiences while ensuring efficiency, stability, and compliance as your business grows.

Money in motion
Unlock liquidity and flow of funds by synchronizing transactions, payment systems, and financial networks without compromising speed or security.

Money at work
Unlock a cohesive financial ecosystem and insights for strategic decisions to expand operations while optimizing performance.

fisglobal.com/contact-us linkedin.com/company/fis x.com/fisglobal

Advancing the way the world pays, banks and invests™