A strategic guide for finance leaders

Mastering payment fraud prevention

Get started

Contents

1 Beyond reaction: Building a proactive defense

2 The shifting landscape of payment fraud

3 Uncovering your vulnerabilities: Key challenges in securing payments

4 The technology-driven defense: Your proactive toolkit

5 Building your fortress: Actionable strategies for a resilient framework

6 The future of payment security: Staying ahead of the curve

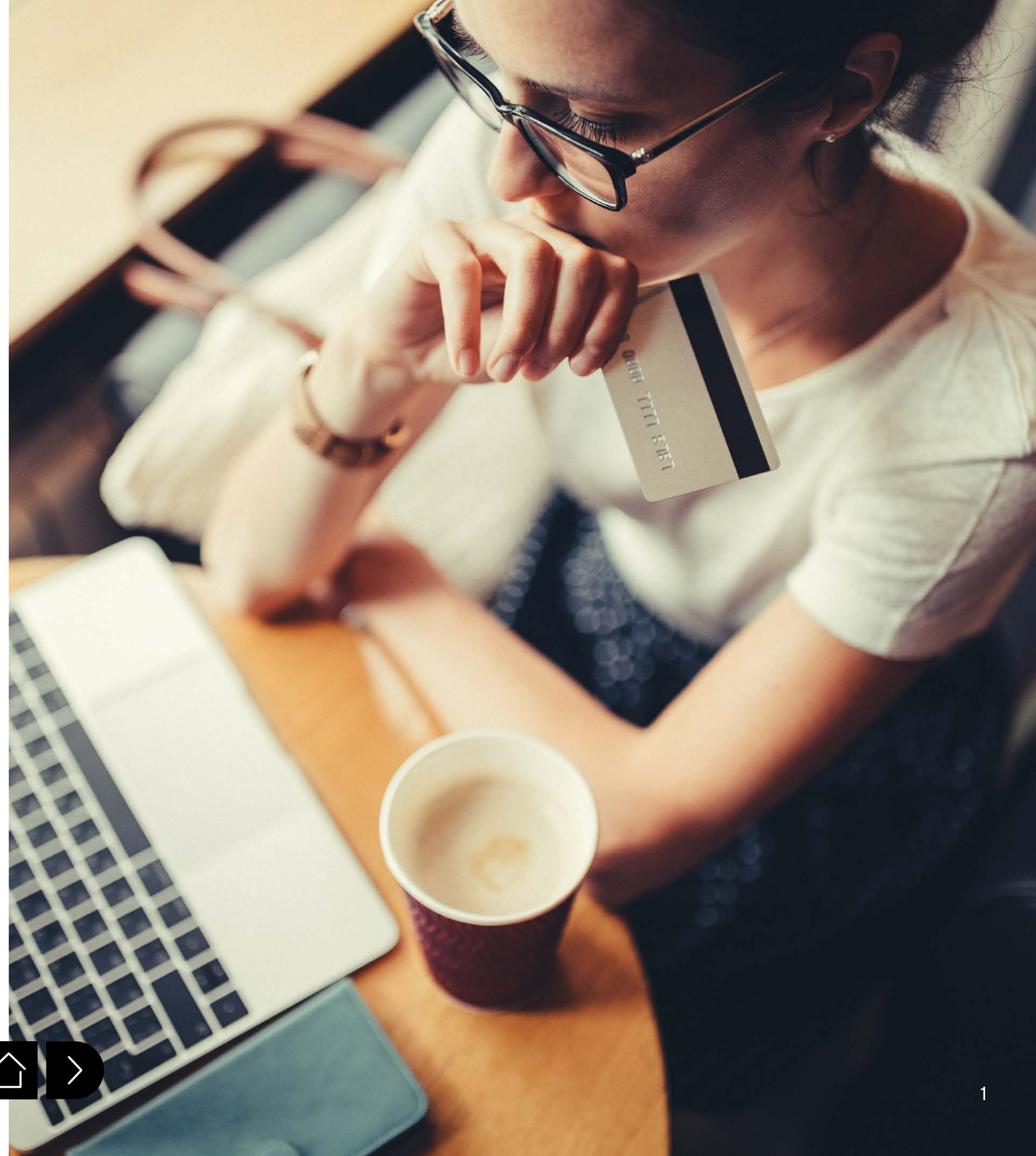
Beyond reaction: Building a proactive defense

Is your organization's approach to payment fraud built for yesterday's threats?

In today's financial landscape, the question is no longer if your organization will be targeted by payment fraud, but when and how. With a staggering 79% of organizations reporting they were victims of payment fraud attacks or attempts in 2024, it's clear that a reactive posture – detecting fraud after it has already occurred – is no longer enough. The very nature of the threat has evolved, demanding a fundamental shift in how finance and treasury leaders approach security.

This e-book serves as a strategic guide for mastering payment fraud prevention. We'll explore the sophisticated tactics used by modern criminals, uncover the key vulnerabilities that exist within your payment processes, and detail the technology-driven solutions that form the bedrock of a proactive defense. Your goal is to move beyond simply managing risk and toward building a resilient framework that protects your assets without sacrificing speed and efficiency.

By the end of this guide, you'll have the insights needed to transform your fraud prevention strategy from a defensive necessity into a strategic advantage.



The shifting landscape of payment fraud

How prepared are you for an adversary that’s organized, well-funded and technologically advanced?

The modern fraudster is not a lone actor operating in the shadows. They’re part of sophisticated criminal enterprises that study organizational charts, identify process gaps, and exploit human psychology with alarming precision. They understand that the entire payment lifecycle – from vendor setup to final reconciliation – presents a landscape of opportunity.

The friction between growth objectives and security risks is palpable. A recent study by FIS® and Oxford Economics found that 75% of C-suite executives identify fraud as a major source of "disharmony" within their organizations. This isn't just an operational headache; it's a strategic challenge that impacts efficiency, reputation and the bottom line.

Criminals are constantly refining their playbook. Business Email Compromise (BEC) remains a dominant and highly effective method, where fraudsters convincingly impersonate executives or suppliers to authorize illicit payments. Now, emerging technologies like AI-powered deep fakes are adding a new layer of complexity, allowing criminals to spoof voices on conference calls to approve transfers. This evolving threat landscape requires a defense that’s equally dynamic and intelligent.

Uncovering your vulnerabilities: Key challenges in securing payments

Where are the weak points in your payment processes that criminals are most likely to target? A proactive defense begins with an honest assessment of your vulnerabilities. For most organizations, these challenges fall into three primary categories.

Securing the entry point: Vendor onboarding

The vendor master file is the heart of your payables process, making it a prime target. If fraudulent bank details are entered into your system, every subsequent payment to that "vendor" is automatically compromised. Criminals often achieve this through sophisticated social engineering, impersonating a legitimate supplier and providing new payment instructions via email. Without strict controls, these changes can be processed, leading to significant losses before the deception is ever discovered.

The oversight gap: A lack of anomaly detection

As transaction volumes grow, manual review becomes both impractical and ineffective. Fraudsters rely on this high volume to hide their activities. A fraudulent payment may be disguised as a routine transaction, slightly different in amount or frequency, but easily overlooked by a human reviewer juggling countless other tasks. Without automated oversight, these subtle deviations go unnoticed until it’s too late.

The human factor: Your first and last line of defense

Your employees are your greatest asset in the fight against fraud, but they can also be your most significant vulnerability. Criminals are masters of psychological manipulation, using tactics of urgency and authority to pressure staff into bypassing established controls. An email that appears to be from the CEO requesting an urgent wire transfer can be enough to trick a well-intentioned employee into making a costly mistake. General cybersecurity awareness is no longer sufficient; specialized, role-based training is essential.

The technology-driven defense: Your proactive toolkit

How can you fight a technologically advanced threat? You need to leverage technology to build an even stronger defense.
A modern, proactive framework is built on a foundation of intelligent and integrated solutions that automate oversight and centralize control.

AI-driven anomaly detection

Moving beyond static, rule-based systems is critical. Solutions powered by artificial intelligence and machine learning establish a baseline of "normal" payment behavior for your organization. These systems analyze transactions in real time, scanning for irregularities that would be invisible to the human eye. Was a payment sent at an unusual time? Is the amount slightly higher than the vendor’s average invoice? AI can flag these deviations for investigation before the funds leave your account, shifting your posture from reactive to preemptive.

Centralized payment hubs

Managing security protocols across disparate ERPs, treasury systems and banking portals creates inconsistencies that fraudsters can exploit. A centralized payment hub provides a single source of truth, offering complete visibility and control over all outgoing payments, regardless of their origin. This allows for the consistent application of security rules, detection analytics and approval workflows across the entire enterprise. It transforms your defense from a series of disconnected fences into a unified fortress.

Account validation services

Before a payment is ever initiated, what if you could confirm the beneficiary is legitimate? Account validation services provide this crucial layer of security. By leveraging vast community databases, these tools verify that the recipient’s name matches the bank account details provided. This simple check significantly reduces the risk of authorized push payment (APP) fraud and protects against simple data entry errors, ensuring funds are sent to the intended party.

Building your fortress: Actionable strategies for a resilient framework

Armed with the right technology, how do you integrate it into a cohesive and effective strategy? Building a resilient framework involves a holistic approach that combines technology, process and people.

1. Sanitize your vendor onboarding and management

Implement a strict, standardized process for adding new vendors and updating existing ones. Mandate out-of-band verification – such as a phone call to a pre-verified contact – before changing any bank account details. Never trust an inbound email request alone.

2. Enforce multi-factor authentication (MFA) everywhere

A password is no longer sufficient protection. Make MFA mandatory for all employees accessing bank portals, payment systems and sensitive financial data. This simple step is one of the most effective deterrents against unauthorized access.

3. Implement layered and segregated approvals

Ensure no single person has the ability to both initiate and approve a payment. Establish clear, documented approval workflows with segregation of duties. High-value or high-risk payments should require confirmation from multiple approvers.

4. Foster a culture of “trust but verify”

Empower your team with specialized training on payment fraud schemes like BEC. Create a culture where it is safe and encouraged to question unusual or urgent payment requests, regardless of who they appear to come from.

5. Conduct regular security assessments

Fraud tactics are constantly changing, and your defenses must evolve in kind. Conduct an end-to-end review of your payment processes at least annually to identify and close security gaps that may have opened up.

The future of payment security: Staying ahead of the curve

The path forward for finance and treasury leaders requires a decisive pivot from reactive measures to a proactive security posture. This isn't just about mitigating risk; it's about building the operational confidence to pursue growth without fear of significant loss.Looking ahead, the regulatory environment is also reinforcing this shift. Upcoming mandates like NACHA's fraud detection requirements in the U.S. and SEPA's Verification of Payee rules in Europe are turning best practices into compliance obligations. Organizations that embrace a proactive strategy now will not only be more secure but also better prepared for the future of payments.

By integrating advanced technology, standardizing critical processes, and fostering a culture of vigilant verification, you can build a fortress around your payments. A secure payment process is the foundation of a resilient, trustworthy and efficient treasury operation, enabling your business to thrive in an increasingly complex world.

Unlock more

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

FIS helps you keep money moving smoothly and at scale.

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.

About FIS

FIS is a financial technology company providing solutions to financial institutions, businesses and developers. We unlock financial technology that underpins the world's financial system. Our people are dedicated to advancing the way the world pays, banks and invests, by helping our clients confidently run, grow and protect their businesses. Our expertise comes from decades of experience helping financial institutions and businesses adapt to meet the needs of their customers by harnessing the power that comes when reliability meets innovation in financial technology. Headquartered in Jacksonville, Florida, FIS is a member of the Fortune 500® and the Standard & Poor's 500® Index. To learn more, visit FISGLOBAL.COM. Follow FIS on LinkedIn, Facebook and X (@FISglobal).

fisglobal.com/contact-us

linkedin.com/company/fis

x.com/fisglobal

Advancing the way the world pays, banks and invests™