Master strategies to deploy in the fight against payment fraud

Unlock a comprehensive defense for the modern treasury

Executive summary

In today's rapidly evolving financial landscape, payment fraud has shifted from a potential risk to an inevitable challenge for organizations worldwide. As transaction volumes increase and payment methods diversify, fraudsters are deploying increasingly sophisticated tactics – from Business Email Compromise (BEC) to deep-fake technology.

This white paper explores the current state of payment fraud, highlighting critical statistics that reveal the scale of the threat. It examines the "disharmony" many organizations feel between their growth objectives and the friction caused by security threats. More importantly, it outlines master strategies for defense, focusing on the integration of advanced technologies like AI and payment hubs, the necessity of regulatory compliance with upcoming NACHA and SEPA mandates, and the critical role of a security-first mindset.

Readers will gain actionable insights into building a comprehensive fraud prevention framework that balances operational efficiency with robust security protocols.

Introduction

Is your organization prepared for the when, not just the if?

For finance and treasury leaders, the question is no longer whether fraud will target their organization, but when and how. The modern payment cycle offers numerous entry points for criminals, from vendor onboarding to the final settlement of funds. As organizations strive for efficiency and speed, they often inadvertently create vulnerabilities that fraudsters are eager to exploit.

The tension – or "disharmony" – between operational goals and security risks is palpable. Recent studies indicate that fraud is not just a technical issue, but a strategic concern that impacts how organizations function and grow.

This white paper serves as a guide for decision-makers looking to master strategies to fight payment fraud. We'll dissect the current threat landscape, evaluate the tools available – such as payment hubs and AI-driven analytics – and provide a roadmap for implementing a defense that's both resilient and adaptable.

The payment fraud landscape

A state of disharmony

The financial sector is currently navigating a period of significant tension. According to a 2024 survey by FIS® and Oxford Economics involving 1,000 C-suite executives, 75% of respondents identified fraud as a major source of "disharmony" within their organizations. This friction is caused by persistent changes including cyber threats, human error and operational inefficiencies.

This disharmony isn't merely a feeling; it's backed by alarming data. An AFP survey revealed that 79% of organizations were victims of payment fraud attacks or attempts in 2024. While many of these were attempts, the sheer volume indicates that criminals are relentless.

The sophistication of threats

Fraudsters have a playbook, and they're constantly updating it. The threats are not limited to one specific area like Accounts Payable (AP) or Treasury; they target the entire payment process.

- **Business Email Compromise (BEC):** Remains the most common method, where criminals impersonate executives or vendors to request urgent payments.
- **Deep fakes:** Emerging technologies allow fraudsters to use AI to spoof voices or even video on conference calls to authorize transfers.
- **Vendor impersonation:** Criminals infiltrate communication channels to change payment instructions, diverting funds to fraudulent accounts.

79% of organizations were victims of payment fraud attacks or attempts in 2024, according to an AFP survey.

Tools and strategies for fraud prevention

To counter a sophisticated playbook, organizations need a "Payment Security Playbook" of their own. A comprehensive approach relies not on a single tool, but on a layered defense strategy.

1. The centralized payment hub

One of the most effective strategies for securing payments is the implementation of a payment hub or payment factory. Currently, it's estimated that 50% to 70% of large corporations have adopted these models.

- **Visibility:** A payment hub provides a single source of truth, offering visibility across all payment channels (ACH, wire, real-time payments) regardless of the originating system.
- **Standardization:** This allows for consistent detection rules and approval workflows across the enterprise, eliminating the risks associated with disparate systems.
- **Integration:** Hubs can integrate with external fraud tools and sanctions screening services seamlessly.

2. AI and machine learning

While rule-based engines are essential for catching obvious errors (e.g., duplicate payments), they are static. Artificial intelligence (AI) and machine learning (ML) offer a dynamic defense.

- **Anomaly detection:** AI analyzes historical data to learn "normal" behavioral patterns. If a vendor who typically receives $50,000 monthly suddenly receives three payments in a week, or a payment doubles in value, the system flags it as an anomaly.
- **Adaptability:** Unlike static rules, ML algorithms evolve, learning from new data to detect novel fraud tactics as they emerge.

3. Account validation services

Validating beneficiary information is critical before a payment is ever released. Third-party services leverage community databases to score the likelihood that a bank account belongs to the intended recipient. This "pre-validation" step significantly reduces the risk of funds being sent to a mule account controlled by a fraudster.

Regulatory updates you need to know

Regulatory bodies are stepping in to mandate stricter fraud controls, turning best practices into compliance requirements.

NACHA (U.S.)

Looking ahead to 2026, NACHA is introducing significant changes for ACH originators.

- Fraud detection requirement: By June 2026, all non-consumer originators of ACH transactions will be required to have fraud detection processes in place. This includes the capability to validate account information to ensure the intended recipient is legitimate.

SEPA (Europe)

- Verification of payee: Effective October 2025, the Single Euro Payments Area (SEPA) will require instant payment providers to verify that the IBAN matches the name of the beneficiary before a transaction is executed. This measure is designed to combat authorized push payment fraud.

These regulations highlight a global shift toward mandatory account validation and fraud detection, making it imperative for organizations to upgrade their systems now rather than waiting for the compliance deadline.

Building the business case

Creating a robust defense often requires investment, which means building a business case that resonates with leadership. It's not just about ROI; it's about strategic resilience.

Beyond dollars and cents

When defining your fraud strategy, consider the broader business goals:

- Cutting losses: Directly preventing financial loss from fraud.
- Operational efficiency: Reducing the time staff spends investigating false positives or correcting manual errors.
- Reputation management: Protecting the brand from the fallout of a public security breach.

A holistic approach

A strong business case brings together stakeholders from IT, Cybersecurity, Treasury and AP. It positions fraud prevention not as a compliance checkbox, but as a strategic enabler that allows the business to operate at speed without compromising safety.

Actionable recommendations

How can you strengthen your defenses today? Here are five master strategies to deploy immediately.

1. Implement multi-factor authentication (MFA):

Ensure that MFA is non-negotiable for accessing bank portals and payment systems. Relying on passwords alone is a critical vulnerability.

2. Adopt a "trust but verify" culture:

Employee training is your first line of defense. Conduct regular, specialized training that goes beyond general cybersecurity to cover specific payment fraud scenarios like BEC. Empower staff to question urgent requests, even from senior executives.

3. Sanitize vendor onboarding:

The entry point of data is often the entry point of fraud. Implement strict controls for vendor setup. Require out-of-band authentication (e.g., a phone call to a known contact) for any changes to vendor bank account details.

4. Leverage technology for anomaly detection:

Move beyond manual checks. Utilize software that can scan for transaction anomalies – such as unusual timing, frequency or amounts – in real time before payments are released.

5. Conduct regular payment assessments:

Criminals escalate their attacks; your defenses must escalate in kind. Conduct an end-to-end review of your payment processes at least every other year to identify gaps that may have opened up due to new technologies or process changes.

Conclusion

The fight against payment fraud is continuous. As fraudsters leverage technology to become more efficient, organizations must do the same. By moving toward centralized payment hubs, embracing AI-driven analytics, and staying ahead of regulatory curves like NACHA and SEPA, treasury and finance leaders can build a fortress around their payments.

The goal is to transform the "disharmony" of fraud risk into the confidence of a secure, resilient financial operation.

Key takeaways:

- Mindset: Fraud is a strategic threat requiring a strategic response, not just a technical fix.
- Technology: Integrate payment hubs and AI to automate detection and reduce reliance on manual processes.
- Purpose: Security enables speed. A secure payment process allows the business to grow without fear of significant loss.

References:
1. FIS and Oxford Economics. (2024). Global C-Suite Survey on Organizational Disharmony.
2. Association for Financial Professionals (AFP). (2024). Payments Fraud and Control Survey.
3. Modern Treasury. (2025). The State of Payment Operations.
4. Webinar Transcript: Master Strategies to Deploy in the Fight Against Payment Fraud. (Speakers: Rob Hansel, FIS; Maria Salazar, PwC; Craig Jeffrey, Strategic Treasurer).