

# Theft & Fraud Prevention

Fraud is no longer a matter of if—it's a matter of when. From business email compromise (BEC) to ransomware, modern threats are more targeted, more professional, and faster-moving than ever before.

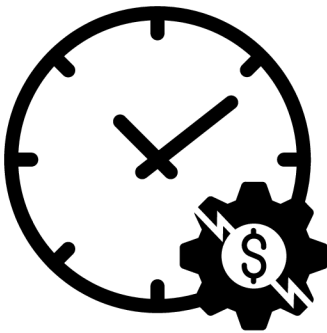
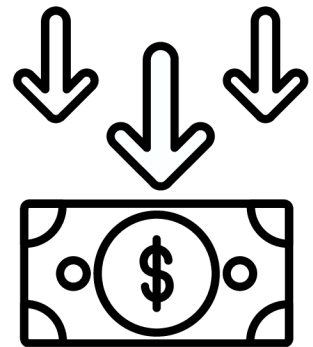


79% of organizations experienced a payments fraud attack or attempt in 2024.

*Source: 2025 AFP Payments Fraud and Control Report*

\$2.7 billion in reported losses from BEC scams (FBI IC3 Report, 2024).

*Source: FBI IC3 Report*

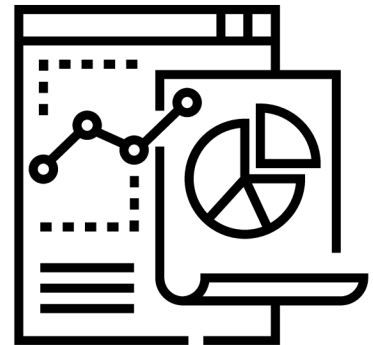


18 days average downtime after a ransomware attack.

*Source: 2025 AFP Payments Fraud and Control Report*

92% of victims who pay ransom don't get their data back.

*Source: InvenioIT Ransomware Report*



## Common Types of Fraud

- **Business Email Compromise (BEC):** Fraudsters impersonate executives or vendors via lookalike domains (e.g., jane.doe@c0rpay.com) to request wire or ACH transfers.
- **Account Takeover:** Attackers gain access to legitimate accounts and initiate unauthorized transactions.
- **Vendor Impersonation:** Scammers pose as suppliers, requesting bank account changes or fake invoices.
- **Phishing & Ransomware:** Emails designed to steal credentials, install malware, or encrypt systems for ransom.

## Practical Prevention Steps

### For Finance & AP Teams

- Use Positive Pay to stop counterfeit checks before they clear.
- Require multi-factor authentication (MFA) for all payment approvals.
- Verify vendor changes through a known phone number, never just email.
- Limit access to financial systems and rotate job responsibilities.
- Use one-time-use virtual cards backed by Mastercard for vendor payments.

### For IT & Leadership

- Implement spam filtering and whitelisting tools.
- Keep systems patched and conduct penetration testing regularly.
- Run phishing simulation training for all employees.
- Develop and test an incident response plan—before you need it.

## Key Takeaway

As long as there's money and valuable data, there will be fraud attempts. The key is layered protection: policies, people, and technology working together.

