PayToMe.co Shares Five Ways Businesses Can Reduce Payment Fraud Risk in 2026

AI-powered fintech platform shares five practical strategies to help businesses strengthen payment security and reduce payment fraud in 2026.

PALO ALTO, CA, UNITED STATES, August 3, 2026 /EINPresswire.com/ -- PayToMe.co, an award-winning AI-powered fintech platform providing embedded finance, Text-to-Pay, and payment automation, today released five practical recommendations to help businesses strengthen payment security and reduce fraud risk in 2026.

> Payment fraud is evolving with AI. Strong internal controls, secure technology, and trusted verification help businesses reduce risk and build customer trust."
>
> *PayToMe.co*

Payment fraud continues to evolve as criminals increasingly use business email compromise, impersonation, fraudulent payment instructions, compromised accounts, deepfake voice technology, AI-generated communications, and social engineering to target organizations of every size.

According to the 2026 Association for Financial Professionals (AFP) Payments Fraud and Control Survey, 76% of organizations experienced attempted or actual payment fraud during 2025. The survey also identified business email compromise as one of the leading payment fraud threats while highlighting the growing use of AI-enabled voice and video impersonation.

Federal Trade Commission data further demonstrate the increasing scale of impersonation fraud. Consumers reported approximately $3.5 billion in losses to imposter scams during 2025, including nearly $1 billion involving scammers impersonating legitimate businesses. Total reported fraud losses reached approximately $16 billion, representing an increase of about 25% from 2024.

As payment fraud becomes more sophisticated, PayToMe.co recommends that businesses strengthen both technology and internal controls through the following five best practices.

1. Independently Verify Changes to Payment Instructions

Businesses should treat unexpected requests to change bank accounts, payment destinations, or vendor information as potential warning signs.

Criminals frequently imitate vendors, executives, employees, or customers using compromised email accounts, look-alike domains, or fraudulent communications designed to appear legitimate.

Before updating payment information, employees should independently verify every request using an established communication channel, such as calling a trusted telephone number already on file rather than one provided in the request.

Verification procedures should apply regardless of how urgent or convincing a request appears.

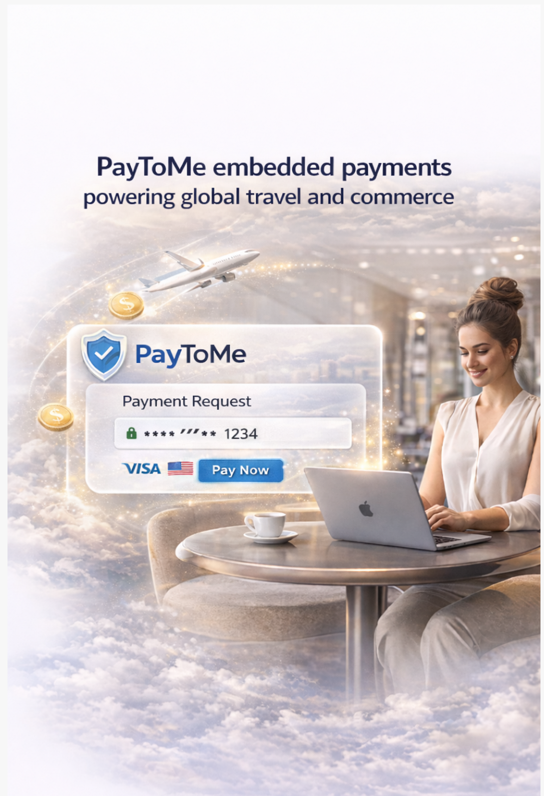
2. Separate Payment Creation and Approval Responsibilities

Allowing one individual to create vendors, modify banking information, approve invoices, and release payments increases exposure to both internal and external fraud.

PayToMe.co - award winning Fintech Platform

Global Partners

Where practical, businesses should separate these responsibilities and require independent approval for higher-risk transactions.



Organizations can further strengthen internal controls by:

Establishing approval thresholds based on transaction size.
Restricting payment-system access according to employee responsibilities.
Reviewing user access whenever personnel change roles or leave the organization.
Requiring additional approvals for first-time or unusually large payments.
Maintaining detailed audit records identifying who created, reviewed, and approved each transaction.

Even smaller organizations can improve oversight by requiring an owner, manager, or external accountant to approve sensitive payment changes.

3. Strengthen Account Security and Protect Verification Codes

The Federal Bureau of Investigation has warned that criminals increasingly impersonate financial institutions through phone calls, emails, text messages, and fraudulent websites to obtain account credentials.

Businesses should:

Use strong, unique passwords.
Enable multi-factor authentication whenever available.
Never share passwords or authentication codes.
Avoid shared user accounts.
Regularly review system access permissions.

Individual user accounts make it easier to monitor activity, investigate suspicious transactions, and strengthen accountability.

4. Reduce Dependence on Paper Checks and Manual Processes

Paper checks continue to be among the payment methods most frequently affected by fraud.

Manual invoice processing can also delay the detection of suspicious transactions.

Businesses should evaluate whether appropriate digital payment workflows can improve efficiency while strengthening internal controls.

PayToMe.co's platform supports:

Online invoicing
Payment links
Text-to-Pay
ACH
eCheck
KYC
KYB
Bank verification

These capabilities help businesses organize payment requests through secure digital workflows while supporting stronger identity verification and payment controls.

5. Create Consistent Payment Communications

Businesses should clearly explain how legitimate payment requests are delivered.

Customers should know:

Which email addresses are authorized.
Whether invoices may arrive by email or text.
Which payment methods are accepted.
Whether employees will ever request passwords or authentication codes.
How to verify suspicious payment requests.

Clear communication helps customers recognize fraudulent payment requests that do not follow normal business procedures.

PayToMe.co's Text-to-Pay, payment links, and digital invoicing help businesses deliver secure payment requests through trusted communication channels while allowing organizations to track delivery, customer engagement, and payment completion.

Preparing for AI-EnabledFraud

Artificial intelligence is making fraud attempts increasingly convincing through cloned voices, manipulated video, realistic emails, and sophisticated impersonation attacks.

Businesses should avoid relying solely on whether communications appear authentic. Instead, verification should always follow established procedures, independent contact information, and appropriate approval controls.

Building a Stronger Payment-Fraud Response Plan

Every organization should establish a documented fraud response plan before an incident occurs.

The plan should identify who employees must contact when suspicious payments or compromised accounts are detected, including financial institutions, payment providers, cybersecurity professionals, legal counsel, and law enforcement.

Responding quickly may improve the likelihood of stopping fraudulent transactions or recovering funds.

Businesses should regularly review fraud-prevention procedures as payment technologies, staffing, and criminal tactics continue to evolve.

PayToMe.co is an award-winning, AI-native fintech platform that powers embedded payments, digital commerce, and intelligent financial infrastructure for businesses worldwide. The platform enables organizations to securely accept, send, request, and manage payments through online invoicing, Text-to-Pay, payment links, ACH, eCheck, KYC, KYB, bank verification, and payment automation.

Built with an API-first architecture, PayToMe.co supports businesses across multiple industries, including travel, logistics, storage, e-commerce, online shopping, global shipping, and enterprise services. Its scalable technology helps organizations streamline payment operations, improve customer experiences, strengthen payment security through secure digital workflows, and accelerate business growth.

PayToMe.co also powers a growing ecosystem of digital commerce platforms, including LuggageToShip.com, ShipToBox.com, and ShipAndStorage.com, bringing together AI, payments, logistics, and commerce into one connected digital platform.

For more information, visit www.PayToMe.co

PayToMe.co
PayToMe.co
+1 650-963-4969
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X
