

# HOW TO STOP PAYMENT FRAUD BEFORE IT HAPPENS

THE AP MANAGER'S 2025 PLAYBOOK

**In 2023, payment fraud attempts spiked 73%.**

**Of the attempts that succeeded, 36% resulted in financial losses of at least \$1 million.**

# How to Stop Payment Fraud Before It Happens

01 Introduction: The Evolving Fraud Landscape

02 Understanding Modern Payment Fraud

03 Your Prevention Toolkit: Strategies That Work

04 AP Automation: A Strong Defense Against Payment Fraud

05 Payment Fraud Red Flags Checklist

06 Conclusion: Fraud Prevention Starts with AP Teams



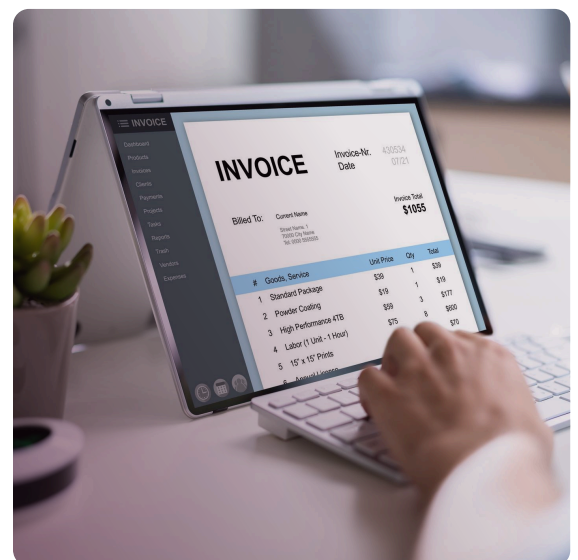
It's 3:45 p.m. on a Friday, and Lisa, an AP manager at a mid-sized manufacturing company, is rushing to finish payments before the weekend. Her phone rings. The caller ID shows her CFO's name. The familiar voice on the line sounds urgent.

"Hey Lisa, I need you to process a wire transfer for a confidential acquisition. It must go through today, or we risk losing the deal. I'll forward you the banking details now. Just process it quickly. No need to run it through the usual approvals. Got it?"

Lisa hesitates. The request is unusual, but the voice is unmistakable. She opens the email with payment instructions and starts keying in the details. But then she remembers something from a recent fraud training: deep fake voice scams.

Instead of rushing, Lisa uses Microsoft Teams to message the CFO directly. A few minutes later, he replies: "I never made that call."

Lisa's quick thinking just saved her company \$250,000.



# Introduction: The Evolving Fraud Landscape

## Today's Payment Fraud Reality

Payment fraud isn't new, but it's never been more sophisticated. In 2023, payment fraud attempts spiked 73%. Of the attempts that succeeded, 36% resulted in financial losses of at least \$1 million.

The uncomfortable truth is that payment fraud has evolved dramatically. While check fraud remains common (increasing 400% in 2023), we're now seeing threats that would have seemed impossible just a few years ago:

- AI-generated deepfake calls mimicking executives' voices
- Sophisticated email compromises that monitor communication for months before striking
- Vendor impersonation schemes with near-perfect documentation
- Attacks specifically targeting instant payment systems like FedNow



What makes these attacks particularly dangerous is their timing. Fraudsters know exactly when to strike. They'll exploit month-end closing, tax seasons, or when your team is short-staffed. They've studied your payment patterns and vendor relationships, sometimes for months, waiting for the perfect moment. AP departments make particularly attractive targets because they:

- Process high-volume, high-value transactions
- Work under deadline pressure
- Maintain relationships with numerous vendors
- Often rely on email for payment instructions
- Frequently handle urgent payment requests



The good news? With the right knowledge, processes, and technology, you can stay ahead of these threats.

In this guide, we'll show you exactly how sophisticated payment fraud works in 2025, the red flags that give it away, and the specific steps your AP team can take to protect your organization.



# Understanding Modern Payment Fraud



## Business Email Compromise (BEC)

Today's payment fraud schemes combine sophisticated technology with clever social engineering. Let's break down the most prevalent threats targeting AP departments in 2025.

BEC attacks remain the most expensive form of payment fraud, costing businesses over \$55 billion during a ten-year period. These schemes have evolved from simple email spoofing to complex, long-term operations.

**Example:** A large construction firm received what appeared to be a legitimate email from their steel supplier. The message referenced specific project details, including the correct purchase order numbers. It was sent from an email address nearly identical to their vendor's actual domain (steelsuppliers-corp.com instead of steelsupplierscorp.com). The email requested updating payment instructions for an upcoming \$293,000 invoice.

The message arrived during the company's busiest season. It referenced real project timelines and even matched the usual communication style of their vendor contact. Only a careful domain check and verification call prevented the payment from being redirected.

### How BEC works in 2025:

- ◎ Fraudsters gain access to email systems and monitor communications for weeks or months
- ◎ They learn payment cycles, project timelines, and communication patterns
- ◎ They strike during predictable busy periods when verification might be rushed
- ◎ They create emails that perfectly mimic legitimate vendor communications
- ◎ They often use pressure tactics, creating a false sense of urgency

# Understanding Modern Payment Fraud



## Vendor Impersonation Schemes

These attacks have become more sophisticated, with fraudsters creating convincing company profiles, websites, and documentation.

**Example:** A healthcare organization received new vendor paperwork from what appeared to be a medical supply distributor. The documentation looked flawless: complete with tax ID numbers, insurance certificates, and business references. The AP team processed a \$76,000 payment for supplies, only to discover later that the entire vendor profile was fabricated. The tax ID actually belonged to a legitimate but unrelated business, and the bank account was controlled by fraudsters.



### How vendor impersonation works:

- ◎ Creation of professional-looking company documentation
- ◎ Minor variations of legitimate company names
- ◎ Use of real business licenses or tax IDs belonging to different entities
- ◎ Temporary but convincing websites that disappear after payment
- ◎ Manipulation of publicly available information to create believable profiles

# Understanding Modern Payment Fraud



## AI-Powered Fraud Tactics

AI technology has created entirely new fraud vectors that were impossible until recently.

**Example:** A technology company's AP team received an email from their software licensing vendor requesting updated banking details. The email perfectly matched the vendor's formatting, included correct license numbers, and referenced their upcoming system upgrade discussed only in private online meetings. The AP director was suspicious because it arrived during their fiscal year-end closing, so he called the vendor's finance department directly. The vendor confirmed they never sent the request.

Investigation revealed hackers had used AI to analyze intercepted communications, learning specific technical and financial details to craft a convincing attack that nearly diverted a \$183,000 payment.

All-in Business Email Compromise		
Feature	Traditional BEC	AI Powered BEC
Attack Method	Email spoofing and fake invoices	AI-generated emails
Detection Difficulty	Moderate (domain checks, off phrasing)	High (perfect email style mimicry)
Common Targets	AP teams, CFOs	C-suite, finance teams, AP
Key Defense Strategy	Call verification, domain checks	Multi-layer verification, secure communication channels

### How AI-powered fraud works:

- AI-generated emails mimic writing styles with uncanny accuracy
- Machine learning analyzes your company's payment patterns to time attacks
- AI chatbots automate conversations to respond to verification questions in real-time
- Deepfake video calls can impersonate executives or vendors
- AI tools help fraudsters generate convincing documentation

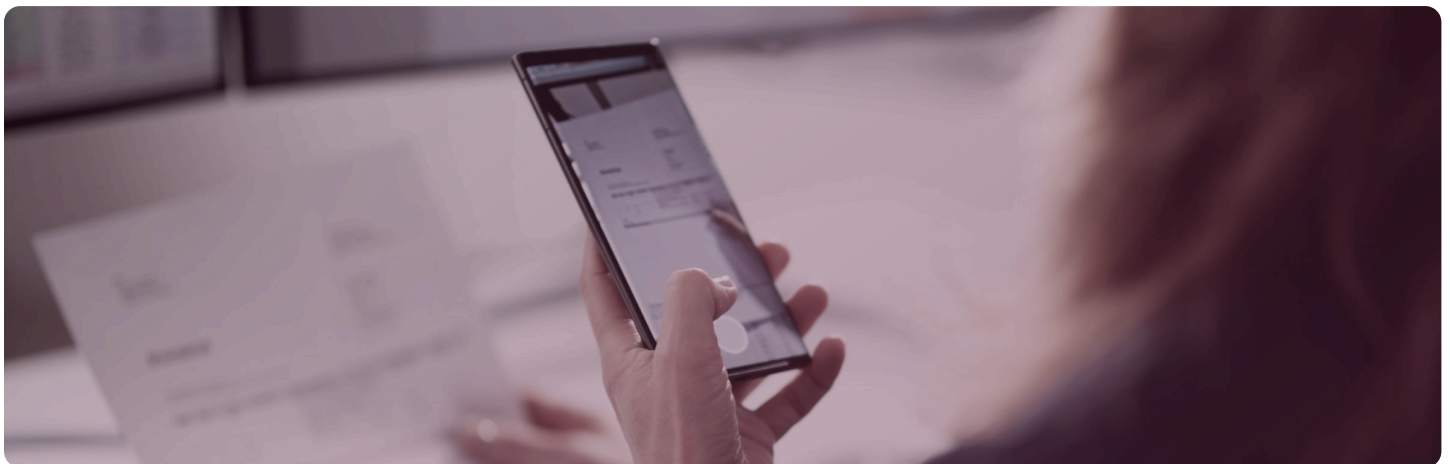
# Understanding Modern Payment Fraud



## Check Fraud

Despite the shift to electronic payments, check fraud remains surprisingly common, with techniques becoming more sophisticated.

**Example:** A finance team thought paper checks were safe until they found thousands missing from their account. Turns out, fraudsters were using simple editing software to change the names on cleared checks while keeping all security features looking normal. These edited checks became templates for creating fakes, showing that even old-school payment methods aren't safe from modern fraud tricks.



### How modern check fraud works:

- ◎ Digital manipulation of check images
- ◎ Chemical washing of physical checks
- ◎ Creation of counterfeit checks using stolen account information
- ◎ Mail theft targeting predictable payment cycles
- ◎ Mobile deposit exploitation



# Understanding Modern Payment Fraud



## Instant Payment Fraud

As FedNow and RTP (Real-Time Payments) have gained adoption, they've created new opportunities for fraudsters who exploit the speed of these systems.

**Example:** An energy company almost lost \$157,000 when a scammer posed as their fuel supplier, claiming there was a payment error that needed fixing right away. The fraudster pushed for immediate payment through FedNow, knowing that instant payments are nearly impossible to get back once sent. Luckily, the company made a quick verification call to their real supplier before sending the money, exposing the whole thing as a scam.



### How instant payment fraud works:

- ⦿ Exploitation of the speed and finality of instant payments
- ⦿ Creation of false urgency to bypass verification steps
- ⦿ Targeting of companies new to instant payment systems
- ⦿ Strategic timing of requests when verification might be difficult

# Understanding Modern Payment Fraud



## Fraud-as-a-Service Trends

Through the dark web, fraud tools are now available to anyone, meaning attacks no longer require technical expertise.

**Example:** A mid-sized retailer experienced multiple sophisticated fraud attempts in rapid succession. Investigation revealed the attacks originated from a non-technical former employee who had purchased access to a "Fraud-as-a-Service" platform. This subscription service provided ready-made phishing templates, fake invoice generators, and even call scripts — complete with coaching from experienced fraudsters.



### How Fraud-as-a-Service works:

- © Dark web marketplaces sell complete fraud kits
- © Subscription services offer ongoing support for fraudsters
- © Templates and tools lower the technical barrier to fraud
- © "Success fees" motivate service providers to help attacks succeed
- © Constant innovation as service providers develop new techniques

**Understanding these modern fraud tactics is the first step toward protection. In the next section, we'll discuss prevention strategies.**

# Your Prevention Toolkit: Strategies That Work

Today's payment fraud schemes combine sophisticated technology with clever social engineering. Let's break down the most prevalent threats targeting AP departments in 2025.

Think of it as a three-step playbook:

1

Spot it early

2

Stop it in its tracks

3

Strengthen your AP workflow

1

## Step 1: Spot It Early

Fraudsters count on slipping past your defenses. They know AP teams are busy and that routine approvals can be rushed. The key to stopping fraud before it happens is knowing what to look for.

### Common red flags in payment fraud:

- ▶ A vendor suddenly requests a change in banking details
- ▶ An invoice arrives with a different format or new contact info
- ▶ A payment request is marked urgent but comes from an unfamiliar source
- ▶ A vendor's bank account is outside their usual country of operation
- ▶ A familiar vendor submits a second invoice with a slightly different amount

It's easy to overlook these small details when processing dozens (or hundreds) of payments a week. That's why automation is so powerful. It catches patterns that aren't obvious at first glance.



### Practical Tip:

Set up automated alerts for any invoice or payment request that deviates from normal behavior. A system that flags these changes can save you from chasing down fraudulent payments later.

# Your Prevention Toolkit: Strategies That Work

## 2 Step 2: Stop It in Its Tracks

Spotting red flags is one thing. Stopping fraud before money leaves your account is another. The strongest AP teams don't just detect fraud. They have built-in safeguards that make it nearly impossible for fraudulent payments to go through.

### Simple ways to strengthen your fraud defenses:

- 🔒 Require multi-person approval for high-risk transactions
- 🔒 Verify vendor details independently before making changes
- 🔒 Call the vendor using a number on file rather than the one in the email request
- 🔒 Use automated fraud detection to compare vendor payment data against known fraud patterns
- 🔒 Restrict payment access to ensure only authorized personnel can approve and execute payments

Many AP teams already have approval processes in place, but fraudsters know how to work around them. Business email compromise (BEC) scams often target senior executives, hoping to pressure AP teams into skipping steps. If a request seems unusual, pause and confirm.



### Practical Tip:

Before approving any vendor payment change, verify the request through a second method. A quick phone call to a known contact can confirm its legitimacy. Fraudsters count on AP teams trusting emails. A simple call can stop a six-figure fraud attempt in seconds.







# Your Prevention Toolkit: Strategies That Work

3

## Step 3: Strengthen Your AP Workflow

Fraudsters look for gaps in your system. The more structured and automated your AP process is, the fewer opportunities they have to slip through. A strong workflow blocks fraud attempts at every turn. It also makes your daily tasks easier by reducing paperwork and eliminating common mistakes.

### Ways to build a fraud-resistant AP process:

-  Centralize vendor payment approvals in one system
-  Automate invoice matching to flag duplicate or altered payments
-  Require regular vendor audits to remove outdated or suspicious accounts
-  Use role-based access controls to ensure only authorized users can make payment changes

Fraud prevention shouldn't slow down operations. The best AP teams create smart workflows that allow payments to move quickly while keeping bad actors out.



### Practical Tip:

Schedule quarterly vendor audits to clean up your vendor list and confirm that all payment details are accurate. Fraudsters often target outdated records because they are easier to manipulate.

## A Prevention Tip That Encourages Teamwork

Here's an effective approach we've seen work: Rather than relying on scattered approvals and manual checks, AP teams implement a quick morning huddle to review payments. This simple process typically takes just five minutes but creates a consistent checkpoint. The key is having a dedicated time when the whole team can spot unusual patterns together.

While these strategies create a strong foundation, the right technology can make your fraud prevention efforts even more effective.

# AP Automation: A Strong Defense Against Payment Fraud

## AP Automation as Your Digital Guardian

Modern AP automation serves as a tireless guardian for your payment process. Here's how it works around the clock to protect your organization:

### Secures Vendor Information

When suppliers request banking detail changes, technology creates multiple safety nets:

- ✓ **Domain verification:** Systems check that emails come from legitimate vendor domains
- ✓ **Secure access requirements:** Changes require login through protected portals
- ✓ **Automatic review triggers:** Banking updates instantly flag for verification
- ✓ **Pattern recognition:** Systems note if vendors recently changed information

### Verifies Every Payment

Smart systems automatically connect the dots between documents, finding discrepancies humans might miss.

When a vendor suddenly changes both their invoice amount and payment details, automated fraud detection can help catch it. Even if the amount seems small enough to normally skip review, the software spots these changes happening together as a warning sign.

### Never-Ending Vigilance

With automation, fraud doesn't slip through the cracks. AP teams use real-time monitoring and smart pattern recognition to stop fraud before it starts. **This constant protection means fewer fraud attempts succeed, saving your company both money and reputation damage in the long run.**

# AP Automation: A Strong Defense Against Payment Fraud

## Before and After: An AP Manager’s Workday

In this chart, learn how automation makes an AP Manager’s job easier and more secure.

AP Task	Without AP Automation	With AP Automation
Processing invoices	Manually checks each vendor’s details	AI Flags unusual vendor changes automatically
Detecting fraud	Relies on employees catching scams	AI-powered three-way matching flags mismatched invoices
Bank detail changes	Requests verified manually	Two-step verification prevents unauthorized updates
Payment approvals	Executives approve via email	Secure portal ensures all approvals are logged

## From Protection to Productivity: The Transformation Story

When organizations implement AP automation, benefits extend beyond security:

**Before Automation:** An AP specialist receives an invoice from what looks like a trusted vendor. The email includes correct purchase order numbers, a familiar logo, and a request to update banking details. The specialist, pressed for time, processes the payment. Two days later, they realized the vendor never sent the request. The company loses \$157,000.

**After Automation:** The same teams can process more invoices with greater confidence. Systems verify transactions automatically. They usually flag only a small number for human review.

Time savings allow teams to focus on strategic activities like negotiating payment terms. And when sophisticated fraud attempts occur, systems can catch them automatically, even with key personnel away.

# AP Automation: A Strong Defense Against Payment Fraud

## Your Technology Roadmap: Where to Begin

You don't need to transform everything overnight. Start your journey with these high-impact steps:

1

Review your current systems for unused security features

2

Implement a secure vendor portal for information updates

3


Add automated three-way matching to your invoice process


4

Consider virtual cards for higher-risk payments

**Remember:** Every upgrade strengthens your fraud defenses without slowing operations. The goal is not perfection. It is to create a system that blocks fraud while keeping AP efficient.

In the next section, we'll explore specific warning signs every AP team should watch for in their payment processes.


 **FRAUD ATTEMPT**




Name

Email

Refunds

 **VERIFIED CUSTOMER**



Name

Email

Chargebacks

14

© 2025 Corpay, Inc. The Corpay logo is owned by Corpay. All third-party marks and/or logos displayed herein are registered ® or claimed ™ trademarks of their respective owners. Corpay respects all trademark rights.

Corpay<sup>^</sup>



# Payment Fraud Red Flags Checklist

Watch for these warning signs when processing payments. If you notice multiple red flags, pause and verify before sending money.

## Vendor Communication Red Flags

- ☐ Email domain is slightly different from the usual vendor domain
- ☐ Request to change bank account or payment details
- ☐ Urgent request for payment that seems out of pattern
- ☐ Request comes during month-end or holiday periods
- ☐ Multiple contact methods that all lead to same person
- ☐ Pressure for immediate payment processing

## Payment Pattern Red Flags

- ☐ Sudden changes in payment amounts for regular vendors
- ☐ Multiple small payments instead of one larger payment
- ☐ Payment amount just under approval thresholds
- ☐ Unusual payment timing for regular vendors
- ☐ Request to change payment method (like check to wire transfer)

## Vendor Setup and Changes

- ☐ Perfect documentation from a brand new vendor
- ☐ Banking country doesn't match vendor's business location
- ☐ Multiple vendors sharing similar bank account information
- ☐ Change in vendor payment information right before scheduled payment
- ☐ Request to send payment to a different address

## Vendor Setup and Changes

- ☐ Perfect documentation from a brand new vendor
- ☐ Banking country doesn't match vendor's business location
- ☐ Multiple vendors sharing similar bank account information
- ☐ Change in vendor payment information right before scheduled payment
- ☐ Request to send payment to a different address

**Remember:** The presence of one red flag doesn't always indicate fraud, but multiple red flags require closer review.

# Conclusion: Fraud Prevention Starts with AP Teams

Payment fraud isn't just a risk. It's a certainty.  
The question is not if fraudsters will try to infiltrate your AP process, but when.

That's why your AP team is the first and best line of defense. With the right safeguards, fraud attempts don't have to turn into fraud losses.

A strong AP process makes prevention seamless. Automation flags suspicious activity instantly. Built-in controls stop fraud before payments leave your account. A structured workflow ensures no fraudulent request slips through the cracks.

But you don't have to do it alone. Corpay's AP automation helps you detect fraud before it happens. You can secure every payment with confidence, reduce manual work, and protect your organization from financial loss.

**See how Corpay makes fraud prevention simple.**

**Schedule a demo today.**

Sources/Research  
[Winter Wonderland or Fraud Land? Protect Your Business | Corpay](#)  
[Fraud Trends & Technology: 5 Inflection Points for 2025 - Nasdaq Veralin](#)  
[Payment Security: Fraud Impact and Prevention](#)  
[Fraud for Hire: Understanding Fraud as a Service](#)  
80% of organizations reported fraud attempts in 2023, a 15% jump in one year:  
[2024 AFP Payments Fraud and Control Survey Report](#)  
recent fraud research: [Ninety Percent of U.S. Companies Experienced Cyber Fraud in 2024, According to New Trustpair Research](#)  
fraud stats: [2024 AFP Payments Fraud and Control Survey Report](#)  
Global payment fraud losses will likely surpass \$50 billion in 2025:  
[Online Payment Fraud: Market Forecasts, Emerging Threats & Segment Analysis 2023-2028](#)  
[Finance worker pays out \\$25 million after video call with deepfake 'chief financial officer' | CNN](#)  
[Payment Fraud Attempts on U.S. Businesses Spiked 71% in 2023, According to New Trustpair Research](#)  
[Internet Crime Complaint Center \(IC3\) | Business Email Compromise: The \\$55 Billion Scam](#)

