FINTWIST
by Corpay

PROTECTING YOUR PAYROLL

A Modern Guide to Preventing Fraud in 2025

Protecting Your Payroll

A Modern Guide to Preventing Fraud in 2025

The 2:00 AM Call

Olivia had been the payroll administrator at a manufacturing company for eight years. She took pride in her accuracy and the trust her 270 employees placed in her to deliver their paychecks on time. That trust vanished at 2:17 AM on a Tuesday, when her phone rang.

"Olivia? This is Victor from IT security. We've spotted unusual activity in the payroll system."

Her stomach dropped. 14 employees had their direct deposit details changed. $42,000 – gone. She had personally reviewed every change request. How did this happen? The answer was unsettling: an AI-generated email had perfectly mimicked an HR request, forging approvals she never gave.

Payroll fraud tactics are becoming more sophisticated, making proactive protection more important than ever. Consider this:

- 10% of all occupational fraud involves payroll schemes
- The typical payroll fraud continues for 18 months before detection
- The average incident costs organizations $383,000

In 2025, payroll administrators face numerous threats. Technology that improves payroll efficiency also opens doors for fraud. Traditional payroll scams haven't disappeared. Instead, they've adapted and evolved with the times.

This guide provides specific, practical strategies to protect your organization from both new and traditional payroll fraud threats.

Emerging Payroll Fraud Threats from New Technology

Threat Type	Target	Goal	Red Flags
AI Voice Impersonation	Payroll staff	Emergency payment changes	After-hours calls, urgent requests, slight voice irregularities
Direct Deposit Phishing	System credentials	Access to payroll system	Unexpected login requests, suspicious links, urgent deadlines
Account Takeovers	Employee payments	Redirect legitimate funds	Unusual system activity, unexpected changes, login anomalies
Chatbot Spoofing	Employee self-service	Credential theft	Unusual information requests, unfamiliar interfaces, suspicious links

AI Voice Impersonation

Artificial intelligence hands payroll fraudsters powerful tools. Criminals now use AI to clone the voices of company executives or HR staff, making phone calls that sound remarkably genuine.

These voice scams typically target payroll administrators with urgent requests to change direct deposit information or process emergency payments to new accounts. The sophisticated voice cloning can sound nearly identical to your company leaders.

How criminals use voice cloning fraud:

1. Record brief samples of an executive's voice from public speeches or meetings
2. Use AI tools to create a convincing voice model that passes basic recognition
3. Call payroll staff during off-hours to create a sense of urgency

How to Spot Voice Impersonation

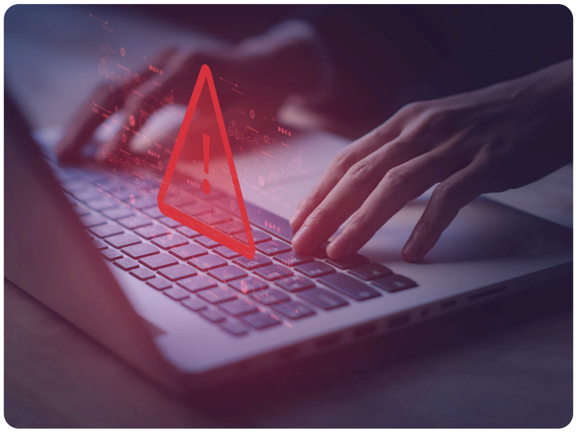
Listen for unusual speech patterns, unexpected pauses, or slight robotic qualities. Be especially wary of urgent calls that come outside normal business hours. Always verify requests through a different communication channel, even when the voice sounds legitimate.

Emerging Payroll Fraud Threats from New Technology

Direct Deposit Phishing

One of the most common payroll attacks starts with a simple email that looks like it's from your payroll software provider:

> *"Your payroll account needs immediate verification. Click here to confirm your login details."*



These phishing attempts use sophisticated techniques, including:

- Perfect copies of legitimate payroll portal login screens
- Company logos and branding taken from your actual website
- Personal information that makes the request look authentic

How to Spot Phishing Attempts

Always check email sender addresses for misspellings or strange domains that signal fraud. Hover over links before clicking to see the real destination URL. Remember that legitimate payroll providers will never email asking for your password or complete account information.

Emerging Payroll Fraud Threats from New Technology

Payroll Account Takeovers

Once criminals have administrator credentials, they don't rush to drain accounts. Instead, they make subtle changes that can go unnoticed for months.

After gaining access, fraudsters typically:

- Change direct deposit information for a small number of employees
- Target employees who check pay stubs less frequently
- Make changes during busy periods like year-end when scrutiny might be lower
- Revert changes after several pay cycles to cover their tracks

How to Spot Account Takeovers

Watch for unusual login times, access from new devices or locations, or multiple failed login attempts before a successful one. Also monitor for unexpected password reset requests or changes to security questions that weren't initiated by the account owner.

Payroll Chatbot Spoofing

As payroll processes become more automated, criminals exploit company chatbots and virtual assistants by creating fake versions of legitimate payroll tools used by employees.

Fraudsters exploit these AI-based payroll tools by:

- Creating fake chatbot interfaces that look identical to your company's legitimate tools
- Manipulating conversations to redirect payroll changes to unauthorized accounts
- Embedding malicious links within seemingly standard chatbot conversations

How to Verify Legitimate Chatbots

Always access payroll chatbots directly through your company's official portal rather than following links. Be suspicious if a chatbot suddenly requests sensitive information it hasn't required before. Verify any unusual chatbot requests through your payroll support team or other secure internal channels.

Traditional Payroll Fraud Risks That Remain Dangerous

While technology creates new threats, classic fraud schemes still cause significant damage. These time-tested scams continue to drain company resources because they work. If you only focus on new threats, you might miss the old ones that still work just as well.

Ghost Employees

Despite advanced payroll systems, "ghost employees" remain a serious threat. These fake employee records funnel money to fraudsters.

In 2025, ghost employee schemes have grown more sophisticated in several ways:

1. Identity Theft: Criminals are now using legitimate Social Security numbers bought on dark web marketplaces.
2. Pattern Matching: They're creating profiles that match typical employee hiring patterns to avoid detection.
3. Timing Exploitation: Fraudsters are adding ghost employees during busy hiring periods when verification might be less thorough.

How to Spot Ghost Employee Fraud

You should regularly review your employee records for several red flags. Look for employees without complete records, multiple employees sharing the same bank account, or employees with no tax or benefit deductions.

Also watch for employees who never take vacation, have no sick leave, or lack performance reviews.

Traditional Payroll Fraud Risks That Remain Dangerous

Prevention in Practice

While leading a post-breach employee audit, Olivia spotted a red flag: an employee with minimal personal information hired during their busy season. This record had no sick leave or benefits, and the direct deposit account matched another employee's banking information except for one digit.

Her investigation confirmed it was a ghost employee created during the previous breach. By implementing regular payroll-to-HR record comparisons, Olivia identified and removed this fraudulent entry before more funds were lost.

Payroll Padding and Overtime Abuse

A longstanding but still prevalent issue, payroll padding involves inflating work hours or falsifying overtime claims. Employees or managers engaging in this tactic may report extra hours not actually worked, often due to poor oversight or manual timesheet tracking.

How Payroll Padding Happens

Payroll padding often occurs through manual entries or by exploiting systems that rely heavily on employee-reported hours. Unethical employees may intentionally clock in early, clock out late, or fail to clock out during breaks.

In some cases, managers collaborate with these employees to approve falsified overtime, sharing in the illicit gains.

Signs of Payroll Padding and Overtime Abuse

Watch for consistent patterns of excess overtime claimed by the same employees month after month. Look for discrepancies between timesheets, reported project workloads, and actual productivity. Be alert to sudden increases in overtime hours without corresponding increases in output or during periods when business is typically slower.

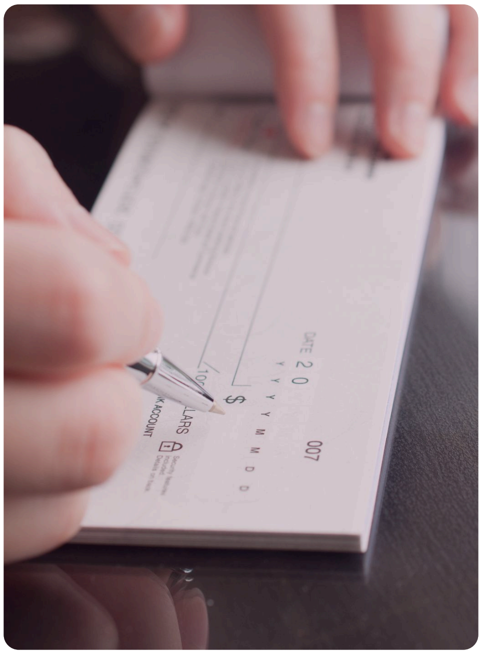
The Hidden Costs of Paper Checks

Malik, a payroll director at a regional retail chain, noticed something odd when reconciling accounts. Three employees claimed they never received their paychecks, yet the checks had been cashed.

After investigation, he discovered the checks had been stolen from their office's outgoing mail and altered using common chemicals to change the payee names.

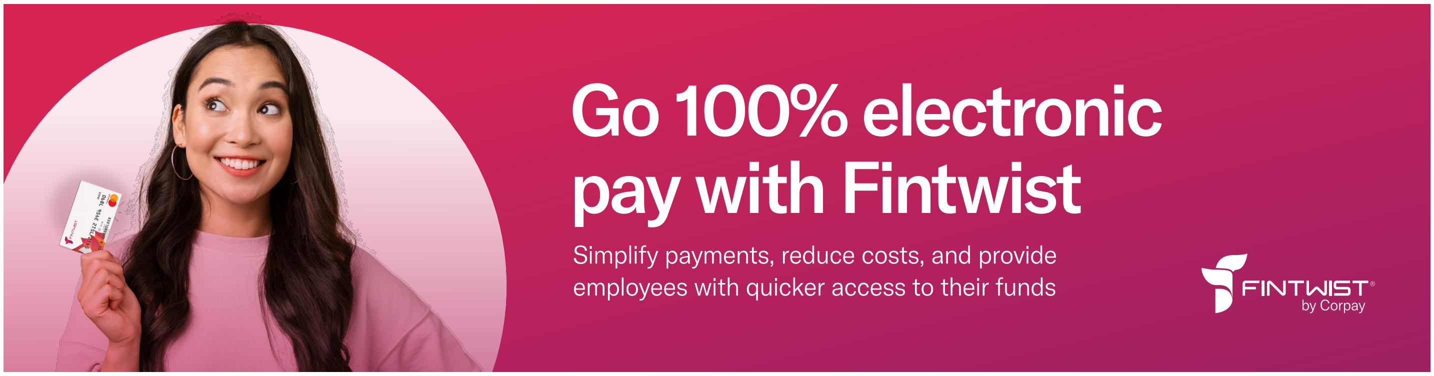
The company spent weeks dealing with police reports, bank investigations, and getting emergency payments to the affected employees. While the actual theft amounted to $4,200, the time and administrative costs far exceeded the stolen amount.

Paper checks create two problems for companies. First, they pose a serious fraud risk, as Malik discovered. Second, they cost money, about $4.40 per check to print, process, and distribute.



Eliminate Paper Check Fraud with Fintwist by Corpay

Malik's check fraud nightmare could have been completely avoided with a digital payment solution. Fintwist by Corpay Paycards provide a secure alternative that prevents check fraud. They also come with enhanced security features and ongoing fraud protection support.


Go 100% electronic pay with Fintwist
Simplify payments, reduce costs, and provide employees with quicker access to their funds
FINTWIST by Corpay

How Fintwist by Corpay Paycards Stop Fraud Before It Starts

Fintwist by Corpay Paycards eliminate paper check fraud risks in several ways:

Fraud Risk	How Fintwist by Corpay Eliminates It
Check Theft	No physical document to steal
Check Washing/Alteration	Digital payments can't be chemically altered
Forgery	EMV chip technology prevents copying
Lost/Stolen Checks	Instant freeze capability if card is lost

If suspicious activity does occur, Fintwist by Corpay's fraud detection team is available 24/7 to freeze accounts, investigate transactions, and provide documentation for any necessary proceedings.

One unique feature of using Fintwist by Corpay's Paycards is that the team works with its clients when fraud occurs. Fintwist by Corpay will assist in communication to team members, and even work with law enforcement to help catch the fraudsters.

Simple Payroll Fraud Solutions To Implement Now

Protect your business with these proven security measures that stop payroll fraud before it happens.

Multi-Layer Authentication Systems

The days of simple passwords are over. Today's payroll systems need multiple verification checkpoints to stay secure.

Strong authentication combines three types of verification:

◎ Something you know (passwords)

◎ Something you have (mobile device)

◎ Something you are (fingerprint or facial recognition)

Most payroll platforms now support authenticator apps that generate time-sensitive codes. These codes expire after 30-60 seconds, making stolen passwords useless without the physical device.

Prevention in Practice

After the breach, Olivia's company implemented multi-factor authentication requiring both a password and a time-sensitive code sent to approved devices. Three months later, the same fraudster attempted to access the system using new phishing tactics to obtain credentials.

While they managed to get a new password, they couldn't complete the second authentication step. This additional security layer successfully blocked multiple unauthorized access attempts, protecting employee payroll data.

Simple Payroll Fraud Solutions To Implement Now

Verification Protocols for Direct Deposit Changes

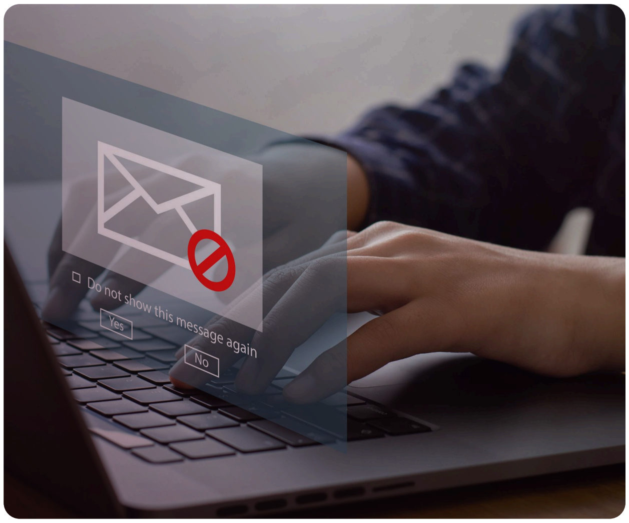
Direct deposit changes represent a high risk in payroll operations. Create a formal verification process that includes these important steps:

1. A 24-hour waiting period between when a change is requested and when it takes effect
2. Confirmation through a different communication channel than the request came from
3. Phone verification using the employee's number on file rather than replying to the email or using a provided number

Prevention in Practice

When Olivia's company updated their security policies, they implemented a three-step verification process. After an employee on parental leave requested a bank account change, Olivia followed the new protocol: she logged the request with a 24-hour processing delay and called the employee's HR-listed phone number.

The employee confirmed the change was legitimate and appreciated the security measure. This simple verification call now protects both the company and employees from unauthorized changes.



Simple Payroll Fraud Solutions To Implement Now

Automated Alerts for Changes

Set up your payroll system to generate automatic notifications when direct deposit information changes or when unusual patterns appear. When employees receive these alerts, they become part of your security team, immediately flagging changes they didn't request.

Quick Tip:
Ask employees to confirm any direct deposit changes by responding to the alert email. This simple step creates a quick feedback loop, helping you catch fraud attempts right away.

Building Strong Fraud Prevention Systems

Now that you've reviewed specific fraud solutions, let's zoom out and explore how to build internal systems that stop fraud before it happens.

Creating Checks and Balances

One of the best ways to prevent fraud is to split up responsibilities. When different people handle different parts of the payroll process, it's harder for someone to commit fraud on their own.

For example, have one person enter data and another approve payments. This works even in small companies. Just make sure any changes to payment information need a second person's approval. This "four-eyes principle" catches mistakes and stops fraud attempts before it's too late.

Simple Payroll Fraud Solutions To Implement Now

Regular Checkups Catch Problems Early

Think of audits like regular health checkups for your payment systems. They help spot issues before they become major problems. Here's what good audit practices look like:

- Match payroll records against HR files to find ghost employees
- Look for duplicate bank account numbers that might indicate fraud
- Confirm former employees no longer receive payments
- Check for unusual patterns that might signal something's wrong

Prevention in Practice

During a routine quarterly audit, Olivia discovered that an employee who had left six weeks earlier was still getting paychecks. The termination hadn't been properly recorded in the payroll system. Her audit caught this error before more money was lost.

Remember that preventing fraud costs much less than dealing with it after it happens. Even small changes to your systems can dramatically improve your security and protect your bottom line.

Quick Tips for Creating a Fraud-Aware Payroll Team

Your staff can spot fraud warning signs that technology might miss. The best prevention happens when everyone knows what to watch for and feels comfortable reporting concerns.

This checklist offers practical ways to involve your team in fraud prevention. These straightforward steps help make security part of your regular workplace conversations rather than an annual training topic.

Train all payroll staff on current fraud schemes

- □ Schedule quarterly fraud awareness sessions
- □ Share examples from your industry
- □ Test knowledge with simulated fraud scenarios

Create a fraud response plan

- □ Document steps to take when fraud is suspected
- □ Assign specific responsibilities to team members
- □ Practice your response through team exercises

Establish a confidential reporting system

- □ Set up an anonymous tip line or email
- □ Create a non-retaliation policy for whistleblowers
- □ Reward employees who identify potential fraud

Build a culture of security awareness

- □ Make fraud prevention part of team meetings
- □ Recognize staff who follow security protocols
- □ Share stories of prevented fraud attempts

Stay informed about new threats

- □ Subscribe to payroll security newsletters
- □ Join industry forums on fraud prevention
- □ Partner with financial institutions for updates

Conduct regular vulnerability assessments

- □ Test your systems for weaknesses
- □ Review processes for potential fraud openings
- □ Update controls based on findings

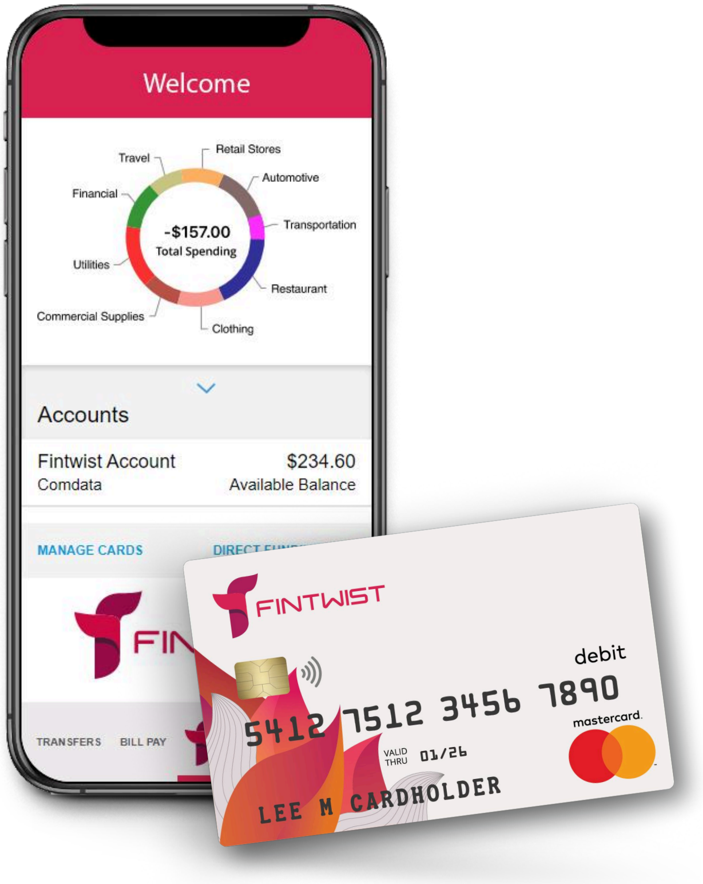
Your Role in Protecting Payroll

As a payroll professional, you stand on the front lines against increasingly sophisticated fraud attempts. The strategies in this guide can significantly reduce your organization's risk exposure.

The impact of payroll fraud extends beyond just financial losses. When fraud occurs, it disrupts operations, damages employee trust, and can harm your company's reputation. With the average incident costing $383,000 and lasting 18 months before discovery, proactive prevention is the smartest approach.

By creating strong verification processes, adopting secure digital payment methods like Fintwist by Corpay Paycards, and building a fraud-aware culture, you can protect both your organization and the employees who count on you for secure, accurate payroll services.

Learn how Fintwist by Corpay's secure payment solutions strengthen fraud prevention and eliminate paper check risks.



Fintwist and Corpay are financial technology companies, are not a bank, and are not FDIC insured. FDIC insurance protects against the failure of the issuing bank (Regions® Bank or Republic Bank & Trust Company), not the failure of Fintwist and Corpay.

The Fintwist Payroll Mastercard® is issued by Regions® Bank or Republic Bank & Trust Company, members FDIC, pursuant to a license by Mastercard International Incorporated and can be used everywhere Mastercard debit cards are accepted. Please see back of card for Issuing Bank. Use of the Card Account is subject to activation, ID verification and funds availability. OnDemand, Bill Pay and P2P is not available for Republic Bank cardholders. Transaction fees, terms, and conditions apply to the use and reloading of the Card Account. See the Cardholder Agreement for details. Standard message and data rates from your wireless provider may apply for use of the mobile app and text message notifications.