

How to prevent fraud in an AI-driven world



Contents

- 3** Fraud costs more than you think
- 4** The characteristics of fraud
- 6** Emerging fraud trends
- 8** The role of technology in fraud prevention
- 9** The human element
- 10** How SAP Concur builds resilience
- 11** Leverage an advanced fraud solution with Concur





Fraud costs more than you think

Fraud is growing more sophisticated—and more expensive—by the day. According to data from Experian, nearly 60% of companies reported an increase in fraud losses from 2024 to 2025.¹

As businesses like yours process payments faster and lean into AI, the risks compound. Hybrid and remote work remove in-person oversight and expand the volume of expense requests. AI makes it alarmingly simple for employees to create fake receipts that human reviewers can't detect. And bad actors can use AI to scale fraud on levels never seen before.

Each case of fraud harms your company, creating financial loss, reputational damage, and an erosion of trust. Businesses worldwide lost an average of 7.7% of their annual revenue due to fraud last year, according to TransUnion data.² For U.S. businesses, that number rose to 9.8%.³

As fraud evolves, so must modern fraud prevention strategies. In this eBook, you'll learn:

- The emerging causes and trends of fraud
- The rising role of AI in fraud detection and prevention
- 5 steps for improving risk management
- How SAP Concur can help you build resilience

¹ Experian, *2026 Future of Fraud Forecast*.

²⁻³ TransUnion, *H2 2025 Update to the Top Fraud Trends Report*, Oct. 8, 2025.

The characteristics of fraud


While a single fraudulent transaction might seem like an anomaly, it's rarely an isolated incident. It often emerges from weak processes or disconnected workflows. This makes it harder to detect patterns of fraud and easier for issues to go unnoticed.

The way your organization manages expenses plays a direct role in reducing fraud risk. Mischaracterized expenses or duplicate submissions happen more often when visibility into travel and expense spend is limited. Without strong controls, small issues compound over time.

Common process-related concerns include:

- Manual workflows that make it easy for intentional errors or expense padding to go undetected
- Rapid growth that makes it harder to spot serial fraudsters who submit small, frequent claims across departments
- Limited visibility that delays detection until audits are conducted, long after the financial leakage happens

4 KPMG, "Fraudsters: usually male, 36 to 55 years old and long-serving employees," May 12, 2025.



Internal controls are insufficient in **76%** of global fraud cases.⁴

A woman with dark hair in a ponytail, wearing a white short-sleeved shirt, is sitting at a desk in a dimly lit office. She is looking at a computer monitor and has her hands on the keyboard. The office has several other desks with computers, and the lighting is warm and focused on the workstations. The background shows glass partitions and a potted plant on a shelf.

FRAUD VERSUS NON-COMPLIANT SPEND: WHAT'S THE DIFFERENCE?

While often grouped due to their impact, fraud and non-compliant spend are separate. Fraud refers to any deceptive spending that is meant to result in a personal benefit, while non-compliant spend is any expenditure that doesn't adhere to your organization's policies or regulatory requirements.

Emerging fraud trends

Deloitte's Center for Financial Services predicts that generative AI could enable fraud losses to reach \$40 billion in the U.S. alone by 2027.⁵ The impact is already being felt across industries. Three-quarters of global business travelers believe it's at least a bit likely that AI is already being used to fabricate expenses, according to SAP Concur research.⁶

FIVE AREAS TO WATCH FOR FRAUD



Deepfake invoices.

AI tools can produce invoices with realistic-looking logos, fonts, itemized entries, value-added tax (VAT) lines, and totals. The most sophisticated tools can even fake or strip metadata, making detection difficult.



Deepfake audio and video.

Bots and tools can mimic a person's likeness with remarkable precision to create fake voice calls and video messages. Most of these tactics rely on familiarity, encouraging employees to approve an out-of-policy expense or bypass normal review steps with a sense of urgency.



Synthetic identities.

Perpetrators combine stolen, legitimate data, such as a real social security or tax ID number, with fabricated names and addresses. They then use those fake identities to open vendor accounts or submit expense reports.



Hybrid work vulnerabilities.

Distributed work models make travel and expense processes decentralized. This can increase the volume of employee-submitted expenses and reduce informal, in-person checks.



Payment fraud and check fraud.

Bad actors gain access to an email account of an employee who makes purchasing decisions, then clone invoices and change the routing number, directing funds into their own account.

⁵ Deloitte, "Generative AI is expected to magnify the risk of deepfakes and other fraud in banking," May 29, 2024.

⁶ SAP Concur, *7th Annual Global Business Travel Report*, 2025.

Fraud trends by the numbers⁷

24%

Scam/authorized fraud

20%

Account takeover

16%

First-party
application
fraud (identity
misrepresentation
or falsified
information)

20%

Synthetic ID fraud

16%

Third-party application
fraud (to open an account)

“

Using the technology to scam people has become so cheap and easy, anyone can do it. That, in a nutshell, is the biggest threat.”

THEODORA LAU, A FINTECH CONSULTANT, SPEAKER AND AI EXPERT


The role of tech in fraud prevention

Intelligent tools can turn travel, expense, and accounts payable (AP) from basic operations into strategic growth. Next-generation technologies that embed these three capabilities can give your business the tools to stop fraud before payment occurs.

AI and machine learning can analyze expense reports, receipts, and credit card transactions to detect fraud in real time. Models trained on large volumes of historical receipts, including confirmed AI-generated examples, can score and flag suspicious images. Continuous retraining keeps detection up to date as fake receipt generation evolves.

Automation. Generating trip-based expense reports automatically removes the errors associated with manual data entry and improves compliance. Embedding policies directly into employee workflows can enable your company to flag non-compliant expenses, such as duplicate receipts or unauthorized vendors, prior to approval.

Advanced analytics. With access to historical spend data, your business can forecast future spend and identify exception-based scenarios, such as mileage padding. Analytics can also spot anomalies in spend data, including outlier transactions and repeated instances of suspicious employee behavior over time.



55% of CFOs expect AI to catch more errors and potential fraud than their team currently does.⁸

The human element

Technology alone won't help your business detect fraud. As you consider leveraging intelligent travel and expense solutions to augment your human reviewers, invest equally in enhancing your audit and compliance teams' ability to catch fraud.

Foster a culture of compliance and ethics.

When compliance is at the heart of your company's day-to-day work, your employees are more likely to act in alignment with company values and expectations. Communicate policies regularly so employees understand acceptable expenses and documentation requirements.

Train employees to recognize and report potential fraud.

Conduct annual training and routine verification so employees remain well-informed about the risks and consequences of fraud. Include modules and workshops that explain the difference between intentional and unintentional fraud, and teach staff where questionable expense claims occur most often.

Balance technology with human oversight.

AI and other tools should augment human work rather than replace it. Automation should help auditors spend more time on resolving risks instead of looking for them. Additional efficiencies should enable staff to focus on investigation, policy review, staff education, and data analytics.



Unsure where to begin?
Try these [Top Tips to Build a Culture of Compliance.](#)

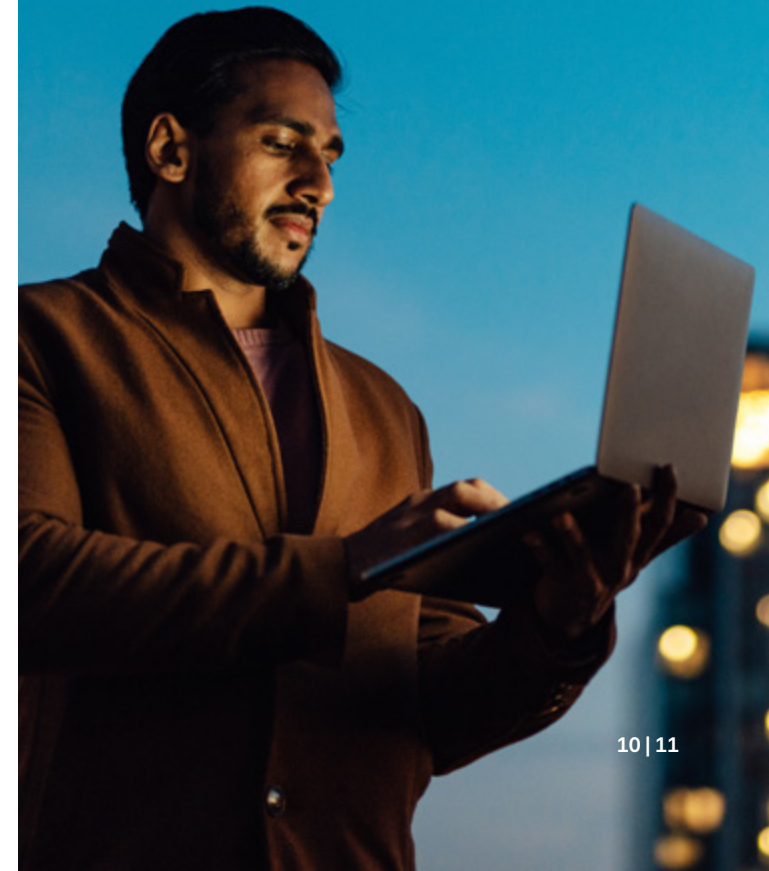
45% of CFOs are concerned that relying solely on technology will allow extra errors to slip through.⁹

How SAP Concur builds resilience

With Concur, your company can implement AI-driven controls to prevent, detect, and mitigate financial losses from accidental errors or fraudulent activity. Our solutions empower you to:

- **Embed policy at every touchpoint to prevent fraud before it starts.** You can add your specific policies into the booking and submission process to guide employee behavior in real time and stop non-compliant spend.
- **Automate expense management and reduce vulnerabilities.** By automating your travel, expense, and invoice management processes, you close the gaps where fraud often hides. This creates a framework of checks and balances that adheres to corporate spend policies.
- **Enable real-time expense creation and notifications.** Provide employees with mobile alerts the moment a card is charged and prompt for missing data instantly. This improves compliance and enables deeper AI automation.
- **Strengthen security with dynamic card management.** Let your finance team lock or unlock cards and apply specific spending restrictions in real time.
- **Gain more control with digital payment cards.** Limit how and where funds can be spent with virtual cards that generate unique 16-digit numbers for single-use or specific timeframes and amounts.
- **Use AI to detect anomalies and flag high-risk transactions.** AI and machine learning can review 100% of expense reports to quickly identify suspicious patterns and high-risk transactions that the human eye might miss.
- **Gain real-time insights and adapt to changing fraud patterns.** Advanced analytics and human audit expertise provide your company with a unified view of spend, enabling you to spot fraud patterns early and stay ahead of emerging risks.

Automated audits reduce the cost of mistakes in expense reports by **60%**.¹⁰



Leverage an advanced fraud solution with Concur

Concur solutions actively prevent and detect fraud as spending happens.

- [Intelligent Audit](#): By combining AI and human excellence, Intelligent Audit scans charges on expense reports, calling out exceptions and flagging those that are potentially falsified or unverifiable. Certified and highly trained human auditors from around the globe then double-check charges that AI could not validate to scan for signs of deepfakes.
- [Verify](#): Simplify your own auditors' workflows and strengthen compliance by embedding policy and receipt checks for in-office and hybrid employees right into Concur Expense. Use AI to detect discrepancies between submitted and established vendor data and flag potential synthetic identities.
- [Concur Detect solution by Oversight](#): With intelligent trend and pattern analysis, plus end-to-end expense audit processes, Concur Detect gives you the visibility and accuracy you need to be confident in every transaction. Expense reports are reviewed against receipts before reimbursement happens, so it's easier to identify anomalies and check for payment fraud.

Learn more at concur.com or at the SAP Concur [blog](#).



enUS (26/02)

© 2026 SAP SE or an SAP affiliate company. All rights reserved. See Legal Notice on www.sap.com/legal-notice for use terms, disclaimers, disclosures, or restrictions related to SAP Materials for general audiences.

Concur solutions empower you to expand reviews throughout the spending and approval process, unveiling trends that may signal spend management issues. This insight enables you to refine your policies for enhanced consistency without overburdening your team.

While you might not know what fraud challenges are around the corner, with Concur, you can take comfort in knowing that you have the robust platform you need.

[Contact us](#) today to discuss how you can prevent fraud for your organization or read a recent [IDC report](#) to discover how customers benefit from Concur solutions to prevent fraud.