INSIGHTS SERIES / CFO

# Combating AI fraud: A guide for finance leaders

How CFOs can lead the fight against AI-driven fraud

SAP Concur

# Finance leaders can spearhead defense against the growing AI fraud threat

AI is now a major driver of fraud. As the technology evolves and criminals hone their tactics, the threat is only set to grow.

Companies report losing

**7.7%**

**of revenue**

to fraud globally

**Source:** Transunion

A recent survey of professionals in finance, audit, and other key functions identified "new technology outpacing controls" as the main driver of fraud.[1] The finding points to a critical moment for CFOs globally as sophisticated new deepfakes and other AI-led scams create profound new risks that are outstripping many finance teams' ability to respond.

In one recent case, a finance worker in Hong Kong erroneously paid $25.6 million to criminals who used deepfake technology to impersonate the company's CFO and other staff during a video call.[2] It's one of several recent episodes in which fraudsters have used AI-manipulated media to cheat people out of money.

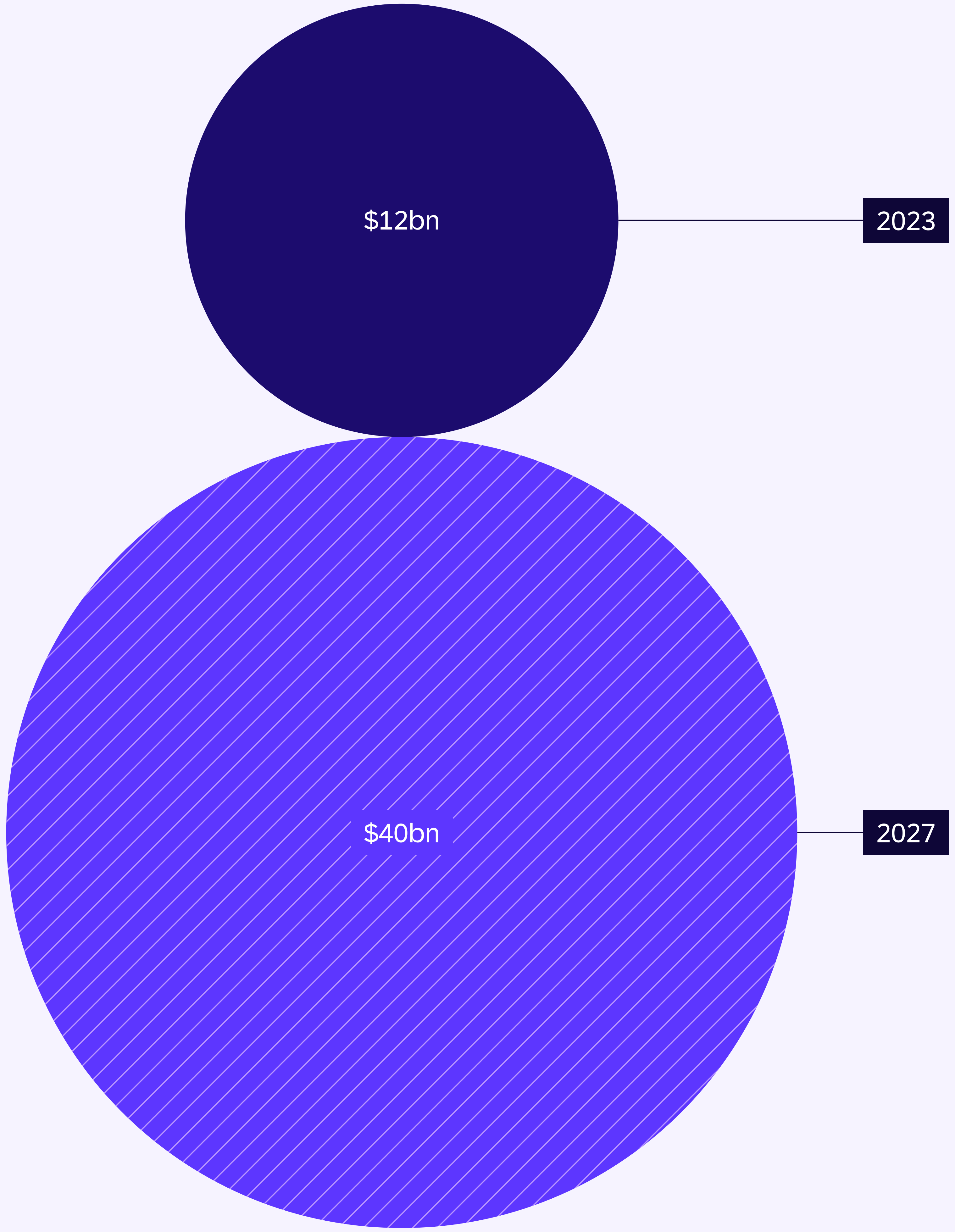
But diligent professionals can fight back, especially when supported with training, tools, and a strong anti-fraud culture. In one instance criminals impersonating the CEO of carmaker Ferrari requested a money transfer from another executive at the company, who foiled the scam by asking a question only the CEO could answer, after which the attacker abruptly ended the call.[3]

## A MORE DANGEROUS ENVIRONMENT

Multiple factors have combined to create a more dangerous fraud environment. These include:

- An increase in attack entry points – such as phones and other remote devices – plus additional software vulnerabilities as enterprise IT systems get more complex and connected
- The democratisation of AI technology, which makes it easier for fraudsters to deploy deceptions quickly
- New attack types, most notably those using AI for impersonation and falsification
- The spread of shadow AI – the unsanctioned use of external tools by employees – which creates extra, low-visibility attack points

**1.** ACCA
**2.** CNN
**3.** MIT Sloan Management Review




$40B

projected losses due to AI-enabled fraud by 2027 in the US alone, up from **$12 billion in 2023**

**Source:** Deloitte Center for Financial Services

"Finance teams need to move beyond reacting to AI-enabled fraud and start designing systems and processes that prevent it. That means **clear, robust policies around the use of pre-approved tools, regular training on AI and fraud awareness** – including how to recognise and verify deepfakes – and a culture where double-checking is normalised. It also means fighting AI-driven fraud with AI itself, using the quality solutions now available."

**Stuart Maclean,**
CFO at Brother UK

$20

starting cost for AI fraud software on the dark web

**Source:** Bloomberg

AI has given new life to older scam methods, such as phishing, which have evolved to become frighteningly convincing – mimicking real people's voices and images, or generating entirely new identities with synthetic documents and fake social media.

Theodora Lau, founder of fintech advisor Unconventional Ventures, says: "I've tested software that creates a fake video of myself cheaply and easily – even my family couldn't tell the difference.

"That realism means new scam types can attack human weaknesses in your controls. Now anyone can get started as an internet fraudster."

Lau predicts the rapid growth in AI-assisted scams[4] will continue as the technology gets ever cheaper and criminals refine their techniques.

All this means it has become harder to predict the next target – will it be payments, expense claims, supplier invoices, or treasury authorisations? Will the threat be external or from the small minority of employees who engage in fraud?

Meanwhile, finance teams are already finding it hard to build strong cyber-defenses. Just 35% of finance teams globally rated their fraud prevention as effective in 2025, a sharp fall from 56% in 2024.[5]

**4.** Experian
**5.** IFOL

# AI fraud: The shape-shifting enemy

Fraud is an elusive target – as soon as finance teams bolster their defenses, criminals pivot to the next weakest link in the human/technology chain.

In a 2025 survey of finance professionals,[6] 77% said scams are increasing, with the most frequently reported activities including business email compromise (BEC), duplicate invoices, and impersonation. This is a rapid shift from 2024, when the main fraud tactics included shell companies and automated clearinghouse (ACH) fraud, alongside duplicate invoices.

## SYNTHETIC DOCUMENT CREATION

Generative AI (GenAI) has transformed document forgery, allowing anyone to fabricate evidence convincingly in seconds. Fake suppliers, receipts, invoices, and travel and expense (T&E) claims are all pathways for fraudsters to extract funds.

The technology can create synthetic data to fill gaps in records or hide discrepancies that make it harder for internal audit teams to detect fraud.

For example, the advent of GenAI has coincided with a sharp rise in falsified receipts[7] and a new wave of AI-generated expenses slipping through checking systems and costing firms millions, according to ICAEW.[8]

## BUSINESS EMAIL COMPROMISE

In BEC scams, criminals impersonate a trusted individual, such as a boss or colleague, to trick someone into transferring money or divulging sensitive information. AI tools now allow fraudsters to scrape public data and LinkedIn profiles to create "life-cycle scams," where the attacker knows exactly when a CFO is travelling or when a specific large contract is due for renewal.

The FBI reported $8.5 billion in BEC losses between 2022 and 2024.[9] Email phishing has expanded to SMS phishing ("smishing") and voice phishing ("vishing"). In all variants, scammers are finding new ways to make attacks more believable by harnessing AI – and this personalisation can be done on an industrial scale.

## AI IMPERSONATION

Deepfake fraud videos – as used in the recent Hong Kong case[10] – rose 20% between 2022 and 2024.[11]

Deepfakes are highly realistic AI manipulations of images, audio, or video that can be used to impersonate individuals, including work colleagues. Notably, the aforementioned Hong Kong case was live via video conference, not prerecorded. This puts real pressure on employees to authorise fake payment instructions or open systems access. A significant percentage of people cannot detect AI-manipulated videos, though they think they can.[12]

This type of scam is escalating rapidly – with worse to come – threatening businesses worldwide, says the European Parliament Research Service.[13]

Most worrying is how these attacks can be combined to create a highly plausible multi-channel attack. For instance, an AI-generated fake invoice could be followed by a deepfake voice note from a credit controller asking for urgent approval.

**55%**

of employees think it's at least somewhat likely colleagues are using AI to falsify travel expense receipts

**Source:** SAP Concur 7th Annual Global Business Travel Report

**47%**

of businesses say they have been defrauded by business email compromise

**Source:** IFOL

**$25.6M**

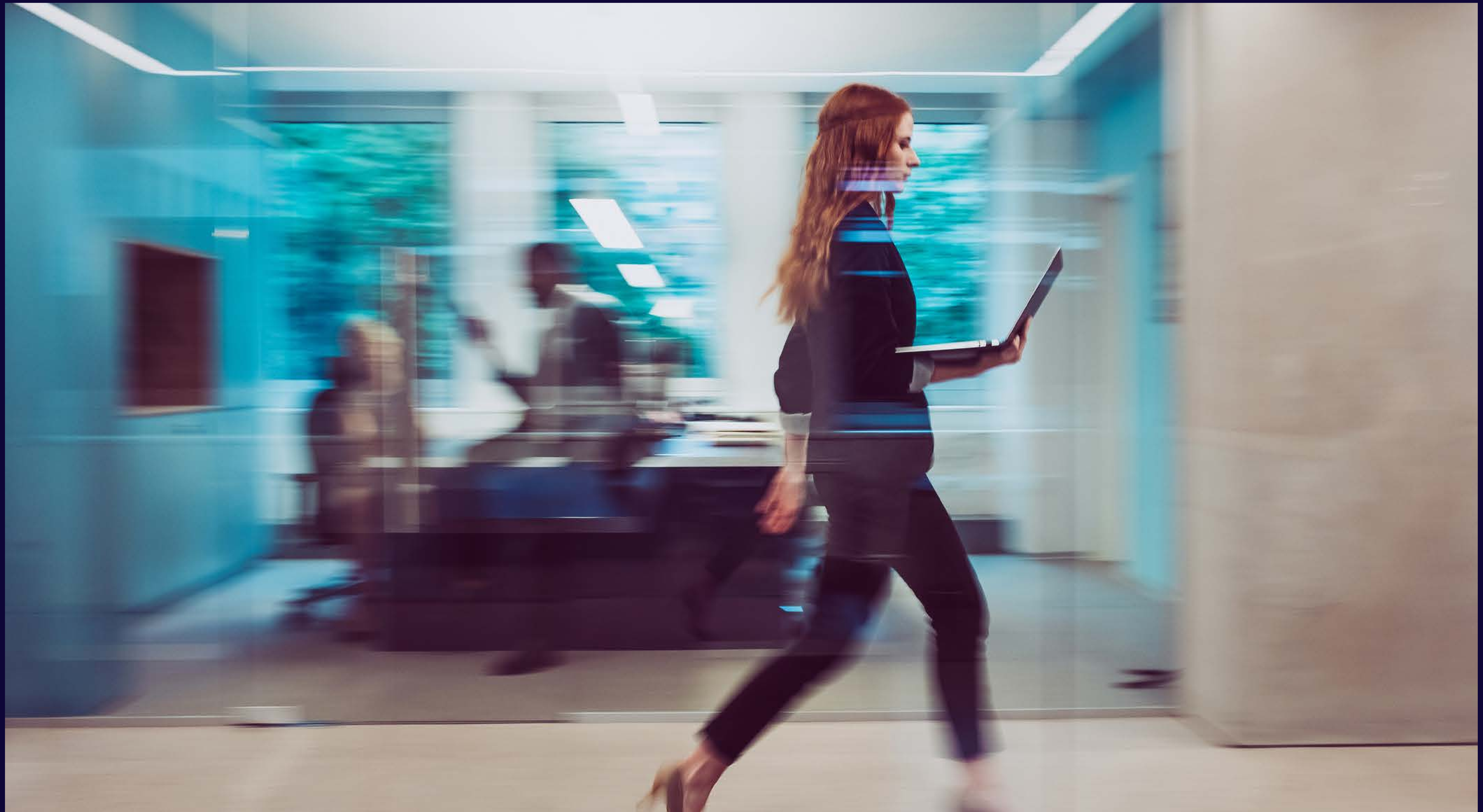
loss to a Hong Kong company after AI scammers deepfaked its CFO on a video call

**Source:** CNN

**6.** SAP Concur
**7.** Financial Times
**8.** ICAEW
**9.** FBI
**10.** CNN
**11.** Regula
**12.** Cell Press
**13.** European Parliament Research Service

# The fightback: People, controls, and governance

AI fraud attacks people's trust, so defending against it is a human challenge as much as a technical one.



In addition to operational controls, finance leaders need governance and people strategies to manage risk effectively. Organisations need a human firewall.

Combating AI fraud should be an all-company initiative. However, the CFO is uniquely placed to take the lead. A good CFO has the technical and storytelling skills needed to drive awareness and change; this also plays into their expanding role in risk management and their ability to unify a response across their own team, IT (technical security), legal, and HR (training).

## OPERATIONAL CONTROLS

CFOs should look at more robust internal controls, including:

- Frequent audits for early detection of irregularities
- Multi-factor approvals for high-value transfers
- Strong dual-control checks for supplier changes
- More robust invoice and expense verification processes – for example, receipt validations that check metadata (such as file type and image data) for suspicious patterns

To sharpen awareness, CFOs should consider simulations that demonstrate how AI-based attacks would work. They should consider adopting CAI standards (cryptographic credentials attached to images, video, audio, and documents) and digital watermarks to make it harder to steal and counterfeit company information.

Proactive data analysis is essential: this correlates with a 50% reduction in fraud duration and losses, according to one study.[14] Companies need a platform that flags issues without a deluge of false positives. In T&E, for instance, this can involve analysing typical spending behaviour patterns and highlighting outliers.

**14.** Commonwealth Fraud Prevention Centre

## GOVERNANCE

Finance leaders need to take AI fraud governance seriously as part of their wider role in cybersecurity oversight. Much of the debate around prevention and detection has so far focused on auditors,[15] but corporate leaders, including CFOs, are responsible for ensuring effective management of the risks.

AI anti-fraud tools are only as good as the governance around them – without strong oversight, AI-based models can hallucinate, embed bias, or expose sensitive data.

To boost governance, finance leaders can consider:

- Shared ownership of anti-fraud models, not internal audit alone, to increase reporting confidence
- Frequent (at least annual) cyber-risk assessments
- Regular reviews of AI controls to reduce attacks in areas such as procurement and accounts payable

Finance leaders must also consider regular checks of their team's ability to prevent the most sophisticated attacks: through predictive analytics, for example. As a further check, they can benchmark anti-fraud programmes against resilience frameworks from organisations such as the Business Fraud Alliance and ACCA.

**15.** ICAEW
**16.** IFOL

## PEOPLE

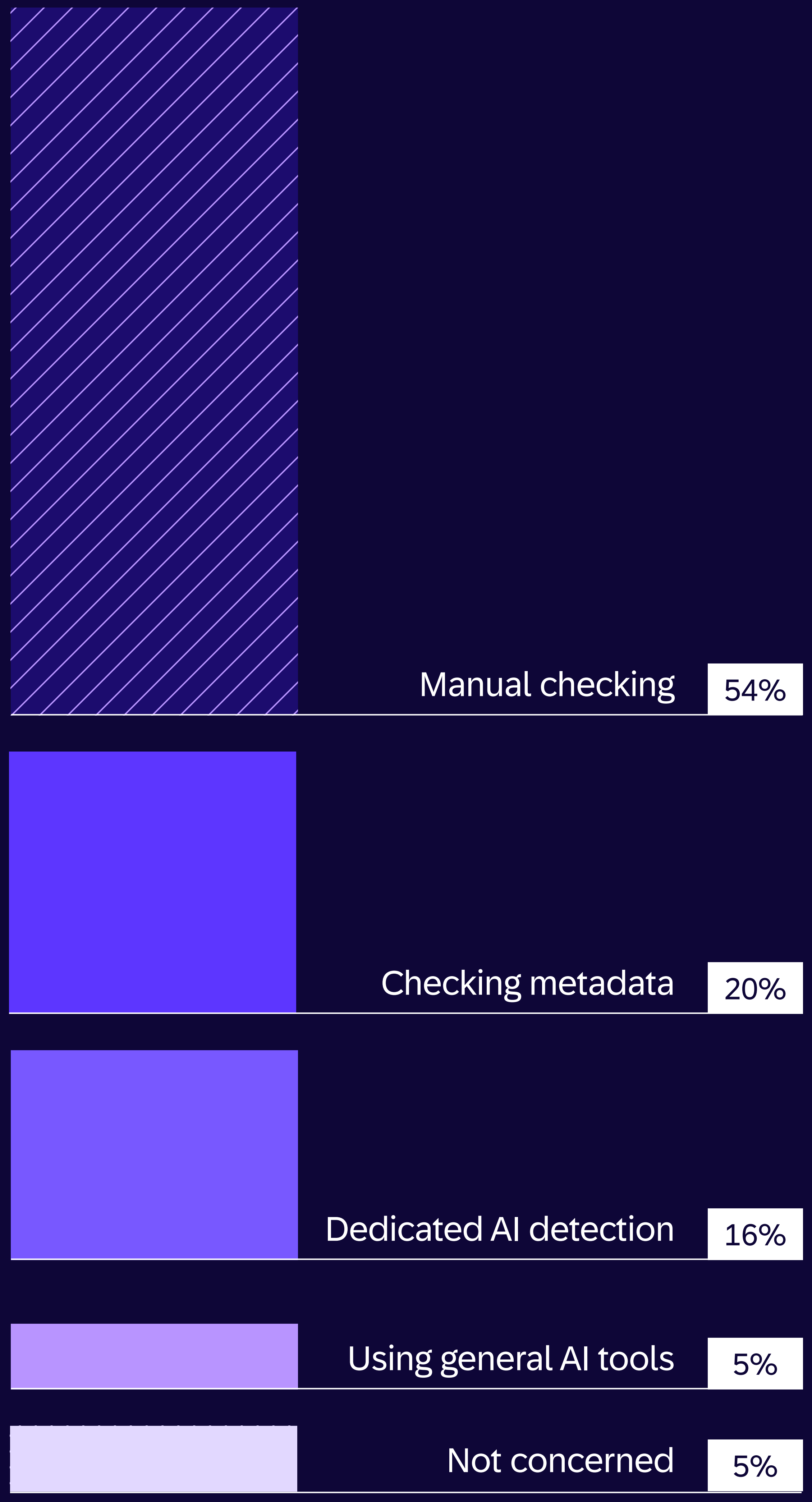
Finance teams are on the front line but say they lack strong support, with some studies showing they feel undertrained and underequipped. Teams rating their fraud prevention measures as "very effective" fell from 56% in 2024 to just 35% in 2025.[16] And 41% believe their manager could do more to protect the team from accounts payable fraud, up from 27% in 2024.

There are many steps finance leaders can take to help their team deal with AI-based threats:

- Train personnel on legal issues such as the EU AI Act and relevant US state and federal laws. Regularly educate them about new types of fraud, such as deepfakes, and about defensive measures, including multi-layer checks, official confirmations, and behavioural risk indicators to flag vulnerabilities.
- Create a fraud-aware culture that encourages curiosity and skepticism. Foster open reporting and candid discussion of mistakes.
- Consider anti-fraud accreditations – for example, staff could train to become a Certified Fraud Prevention Specialist.
- Encourage robust due diligence, applying the same kind of "verify, contextualise, and question" checks that are effective against money laundering.
- Give frontline staff and checkers time to stand back and think about what they're approving. Build a no-blame culture so staff who click on a deepfake link report it immediately rather than hiding it.

Training resources on the latest attack techniques are available from SANS Institute and MIT.

How are firms trying to combat document fraud?




**Source:** Resistant.ai

**Theodora Lau,**
Founder of fintech advisor Unconventional Ventures

"One of the biggest challenges we see is ownership. With the fast-evolving, complex, and interconnected technology landscape, **we need a framework in which everyone is a vigilant risk manager**, not just the person in charge of compliance."

# How AI anti-fraud tools can bolster defenses

## Cognitive technology is supercharging cyber-scams, but it can also be the best defense.

Just **12%**

of firms use AI technologies to ensure compliance or detect fraud in spend management

**Source:** IFOL

AI-powered anti-fraud tools are increasingly effective, provided they go hand-in-hand with the operational and cultural capabilities mentioned above. Over half of CFOs (55%) expect AI to catch more scams than traditional methods, according to SAP Concur research.

Organisations have reported successful use of a range of tools, from behavioural analytics that provide early warning of attacks to solutions that flag suspicious data or spot fake records, such as receipts.

These tools work best when integrated into solutions from trusted vendors. For example, SAP Concur solutions and accompanying best practices can help detect and mitigate fraud, using AI algorithms to strengthen company defenses.

Despite the availability of these tools, 2025 research shows no clear trend toward adopting AI anti-fraud technology – 71% of respondents don't use AI in spend management processes, and only 18% use scam detection software. This lack of investment may expose organisations to preventable losses.

Finance leaders should consider:

- Using AI to detect and flag anomalies and suspicious patterns in real time, combined with people skills to interpret the results
- Deploying tools to help identify deepfakes, such as those from Reality Defender and C2PA, a technical standard that helps prove an invoice or other document has not been altered
- Integrating AI anti-fraud tools with Enterprise Resource Planning (ERP) and other solutions throughout the organisation

**Victor Domingos,**
CFO at SAP Concur

AI disruption is real and affects every function and industry, but it is not just a threat. For finance leaders, it is also a powerful ally. **Used well, AI strengthens fraud prevention, enhances screening and training, improves compliance, and detects patterns humans might miss** – combining human augmented intelligence with better enablement to prevent and spot fraud earlier."

# Find out more

Rising fraud demands smarter financial controls. Read How to Prevent Fraud in an AI-Driven World to strengthen your defences.

## About SAP Concur

SAP® Concur® is the world's leading brand for integrated travel, expense, and invoice management.
Driven by a relentless pursuit to simplify and automate everyday processes, the solutions guide employees through business trips, move authorized charges directly into expense reports, and automate invoice approvals.
By integrating near real-time data and using AI to analyze transactions, businesses can see what they're spending, improve compliance, and avoid possible blind spots in the budget. SAP Concur is imagining a world where travel and expenses practically manage themselves, helping businesses run at their best every day.