Hey! What's New? 2026-49

A Guide to Fighting AI-Fueled AP/AR Fraud

Andrew Kenney writes, in the *Journal of Accountancy*, that "the accounts payable and accounts receivable functions (AP/AR) have long been targeted for fraud, but widely accessible artificial intelligence (AI) is making business scams more convincing, more prevalent and easier than ever to concoct." He adds that "For the modern CPA, the fundamentals of internal controls have never been more critical, or more difficult to maintain. Finance leaders must mount a threefold response to fraud, embracing new technological controls while also sharpening the company's threat awareness and strengthening its dedication to payment best practices."

According to Emily Chee, CPA/CFF/CITP, a senior manager for BDO Canada specializing in forensic investigations, disputes and data analytics, AI is also contributing to internal fraud attempts. "Expense fraud is on the rise, especially with AI," she says. "Most notably, modern software tools have made it trivially easier to doctor receipts and other documents."

"For example, free-to-use websites can produce receipts with vendor names, amounts, and other details selected by the user. A mainstream AI service like Google Gemini can then be asked to edit the image, making it look weathered and photorealistic." And, Chee adds, "modern image editing applications include new AI-powered tools that make it easier to modify documents seamlessly."

Internal fraudsters also may use AI tools to improve and target their attempts, such as by combing through a vendor list to find companies with multiple locations that might easily be impersonated, Clay Kniepmann, CPA/CFF/ABV, J.D., a forensic, valuation, and litigation principal at Anders CPAs + Advisors, points out.

The unifying factor of all these types of scams, says Jonathan Marks, CPA/CFF/CITP, CGMA, MBA, CFE, NACD Board Fellow, a principal in BDO's Forensic Investigations, Disputes and Regulatory Compliance Practice., is that AI is making fraud more accessible. "What AI has done is dramatically lower the competence threshold for some folks. Anyone with a laptop or an iPhone or an Android can run these [scams] now."

What can companies do to protect themselves? "Companies must strengthen their anti-fraud fundamentals, according to the experts interviewed for this article, while also shoring up their cyber capabilities," writes Kenney.

Companies with disorganized vendor records are more vulnerable to fraud attempts of all types — regardless of whether AI is involved. "You want to keep that [vendor list] tidy, you want to keep it as small as possible. And you want a robust vendor setup process to confirm that that vendor's real before you ever set it up in the system," Kniepmann advises.

Companies that maintain strict cash flow controls are more resilient against fraud. According to Kniepmann, "you want two people involved in the step where money comes into the company." In other words, payment processes should be supervised by multiple people. Requiring a second review makes it more difficult for an employee to divert payments and also provides assurance against increasingly convincing external fraud attempts."

According to Ray Sang, CPA/CITP, finance transformation director for cybersecurity company SentinelOne, “organizations must educate employees on the new ways that technology is enabling fraud — while also reinforcing anti-fraud basics. Training is the best control for any organization,” Sang sats. As always, “employees must be taught to recognize suspicious patterns and exercise skepticism, he said. They also should be educated on AI’s capabilities — including through demonstrations of deepfake videos and audio.”

Just as AI has empowered attackers, it also can strengthen defenses. For example, Chee has been using her organization’s closed AI environment to develop bots that can speed her fraud investigations by extracting data from documents *en masse*. “Advancements in technology allow fraud to occur more easily, but the advancements will also allow us to better detect it,” she says. “It’s a double-edged sword.”

Additionally, technological defenses bring ethical concerns, Sang points out. “Powerful new computer monitoring platforms make it easier to track employees’ activity and raise red flags for potential fraud, but excessive oversight may demoralize and outrage workers. [Fraud monitoring] becomes much more accurate and much more meaningful, but now with AI’s help, I do see a trend of centralized [employee] surveillance,” he said.

Fo a whole lot more, see [A guide to fighting AI-fueled AP/AR fraud].