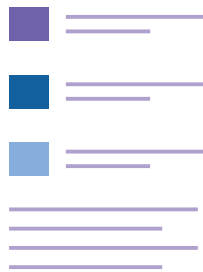
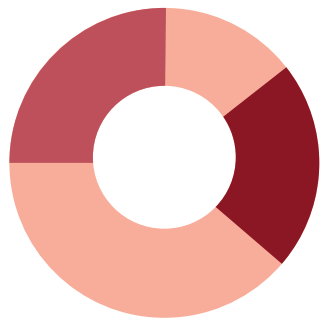


AP Fraud and Security in 2025: Benchmarking the Trends



AP Fraud and Security in 2025: Benchmarking the Trends

IOFM recently conducted a benchmarking survey to explore how fraud is evolving within accounts payable. Of particular interest were factors that appear to influence the frequency of fraud attempts; how long it typically takes organizations to recognize they've been a target of fraudsters; and what steps can be taken to mitigate this type of financial threat.

The survey was conducted in early 2025 with over 350 AP professionals participating. Questions centered around organizations' vulnerability to fraud attempts in the first place, how to recognize them when they do occur and how to prevent them from actually being successful. Comparisons between 2023 and 2024 incidents were made as a means of predicting trends we can expect to see in 2025.

The Evolving Fraud Experience

Before we dive in, it's worth pointing out that survey participants were only able to report those incidents they became aware of. If fraud went undetected — and it's not unreasonable to assume at least some of it did — that data is not reflected in this whitepaper.

Nonetheless, as we see in Figure 1, nearly a third of organizations detected between one and five fraud attempts in 2024. Nearly as many survey participants noted they had been targeted six times or more in that same timeframe. Just fewer than one in five respondents reported no known fraud attempts.

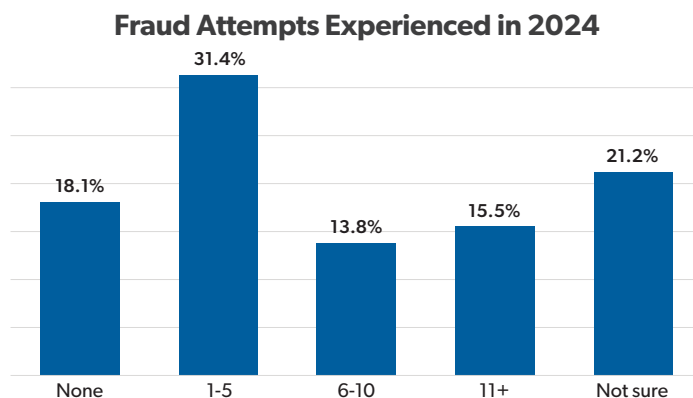


Figure 1. Frequency of Detected Fraud Attempts in 2024

How does that compare to attempted frauds in 2023? Figure 2 indicates that about half of survey participants experienced more fraud attempts in 2024 than they did in 2023. This is likely indicative of things to come, says Shelly-Ann Campbell, S2P Strategic Solution Manager at Esker: "This trend is expected to persist, leading to an anticipated rise in fraud in 2025."

Fraud Attempts in 2024 Compared to Those in 2023

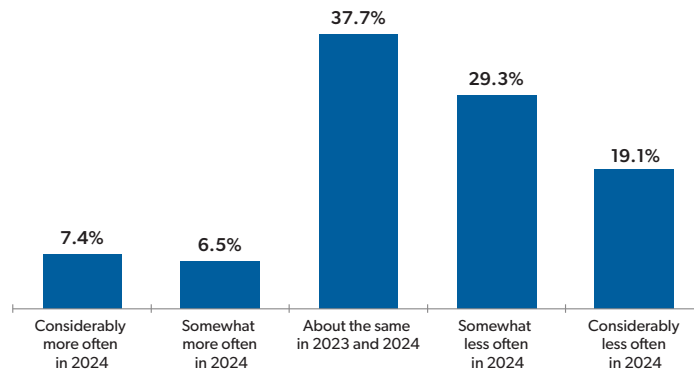


Figure 2. Comparison of Fraud Attempts in 2024 Compared to Those in 2023

In Figure 3, we see the number of fraud attempts that were deemed to be successful in 2024. While six out of ten respondents stated that no attempts were in fact successful, again, it's worth remembering that there may well have been some scams that went undiscovered and were therefore not reported. Three out of ten respondents indicated that between one and five attempts were determined to have been successful.

Number of Successful Fraud Attempts in 2024

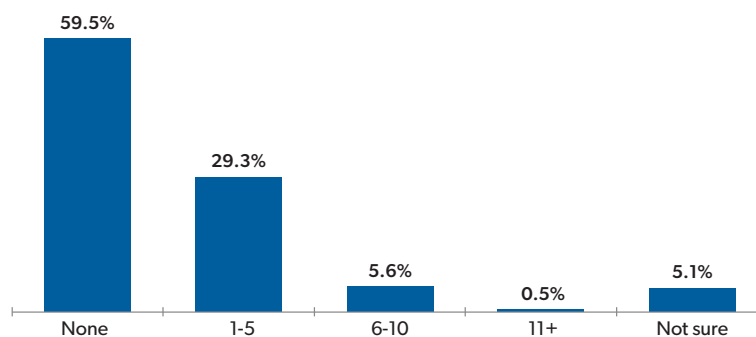


Figure 3. Number of Successful Fraud Attempts in 2024

Fraud Techniques and Targets

Figure 4 shows the types of fraud experienced by respondents. These include:

- **Business email compromise.** These are fake emails that appear to come from a reliable source like a vendor or company executive requesting urgent payments, particularly wire transfers, banking information changes and the like, to trick employees into sending payments to bad actors.
- **Phishing.** Employees receive emails from fraudsters that contain bad links that will direct them to scam websites in order to obtain their login information or other sensitive financial data.
- **Check fraud.** Here, checks are altered or forged to create unauthorized payments.
- **Invoice fraud.** Invoices are rendered for goods and services that were never ordered or provided, or invoices are manipulated to change billing amounts, banking information and so on.
- **Mail interference.** This is theft of paper mail, such as checks.
- **Deepfakes.** These use artificial intelligence to create audio or video simulations of trusted individuals to fool employees into thinking they are talking to an executive or key vendor requesting a rush payment, for example.
- **Ransomware.** This type of fraud attack installs malicious software on an organization's system and blocks access to its data until a sum of money — a ransom — is paid.
- **Internal fraud.** This involves deliberate manipulation of banking information, initiating fake payments, and similar schemes perpetrated by an organization's employees.

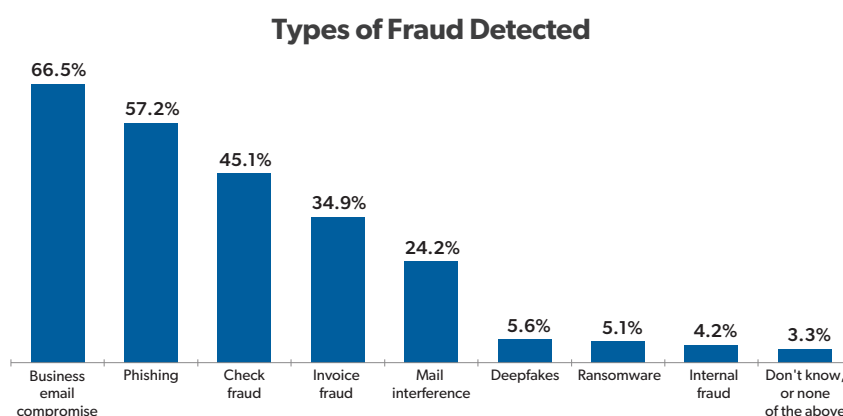


Figure 4. Frequency of Detected Fraud Techniques by Type

Figure 5 reveals the payment types most often targeted by fraudsters: checks. This isn't particularly surprising, given that physical checks are easy to steal, alter and forge. Fraud detection software works to prevent fraud occurring in the first place, but it's only after a falsified check is cashed that it might possibly detect the fraud, and at that point, it could be too late to recover the funds.

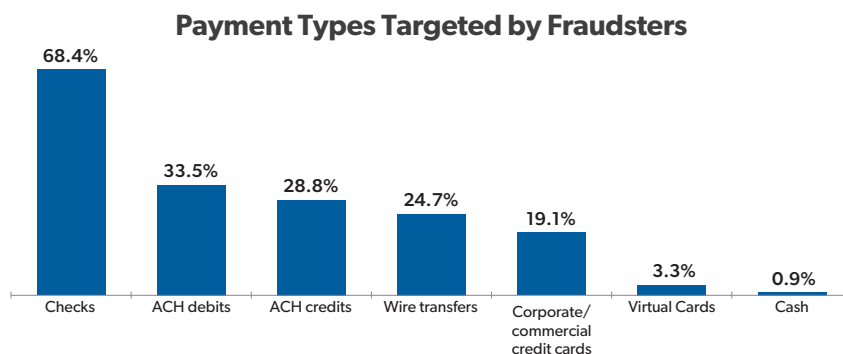


Figure 5. Payment Types Most Often Targeted by Fraud

Rise of Check Payments

This begs the question: How commonplace are check payments these days? While Campbell notes that virtual payments are now dominating the payment landscape, most organizations still make at least some of their payments by check. Figure 6 shows that more than four in ten companies still pay up to a fourth of their invoices by check, and nearly all of them make at least some check payments.

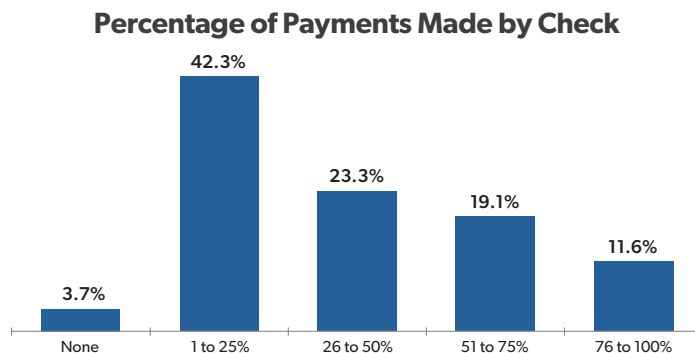


Figure 6. Percentage of Payments Made by Check

It's not hard to infer that if physical checks are the most vulnerable to fraud of any payment type, and the vast majority of companies are still using them at least to some degree, there is a much greater likelihood of them becoming targets than those who only make virtual payments.

Let's look at the math. Figure 7 shows the frequency of fraud attempts based on how often companies make payments by check. Those companies who don't pay by check whatsoever experienced a very low incidence — three-fourths of them reported just five attempts or even fewer in 2024. However, those who make more than half of their payments by check saw a far greater incidence of fraud attempts — double or even more incidents than experienced by those who don't use checks whatsoever.

Number of 2024 Fraud Attempts Based on Percentage of Check Payments

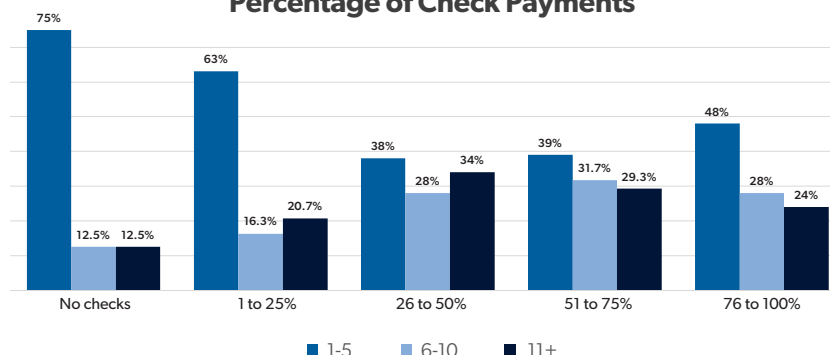


Figure 7. Number of 2024 Fraud Attempts Based on Percentage of Check Payments

How is that trending? As we see in Figure 8, most survey respondents reported that fraud attempts had increased in 2024 as compared to 2023, regardless of their volume of check payments. But those who pay three-fourths or more of their invoices by check saw the biggest spikes last year. That does not portend well for check fraud in 2025.

Comparison of Fraud Attempts from 2023 to 2024 Based on Percentage of Check Payments

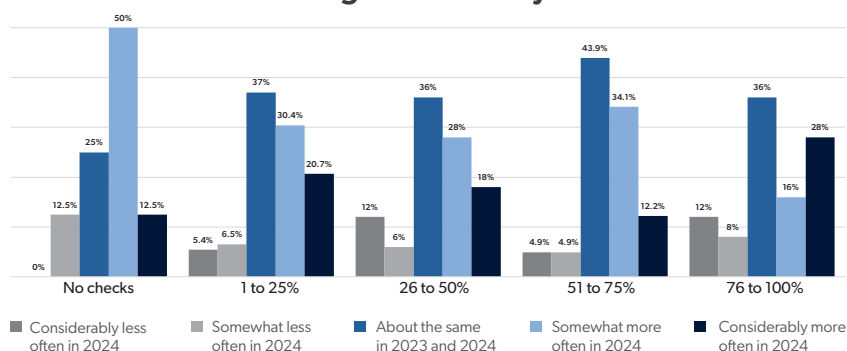


Figure 8. Year-Over-Year Fraud Attempts Based on Check Payments

Fraud Detection and Recovery

How long does it typically take an organization to recognize a fraud attempt? Figure 9 shows that nearly half of respondents knew it immediately. It took about another third of participants several days, but the remainder took weeks or even months to identify the fact that they'd been targeted. Of course, the more time that goes by, the less likely it is that the stolen funds will be recovered. According to the Association for Financial Professionals, a timely filing of a fraud claim with the bank must be made in order to try and recover the funds, and if it takes considerable time to discover the fraud in the first place, it erodes that window.

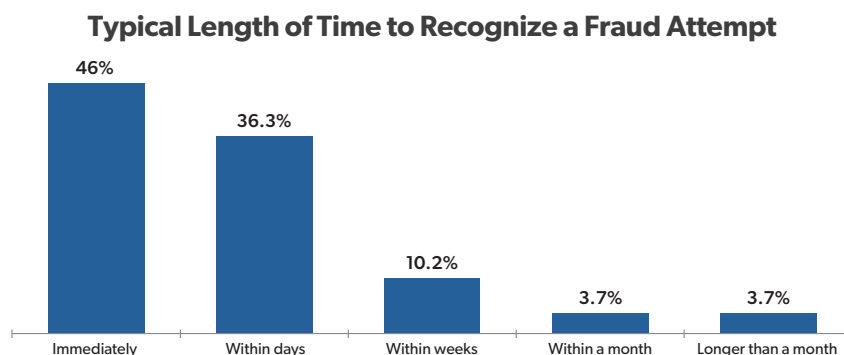


Figure 9. Time to Recognize a Fraud Attempt

However, if the fraud is check-related, does it take longer to discover it? Yes, as shown in Figure 10. Fewer organizations were able to identify it immediately, likely due to the time it takes for checks to clear the bank. Over one in five companies that were victims of check fraud reported it took them weeks or even months to discover it.

Length of Time to Recognize Fraud Attempts for Check Payments

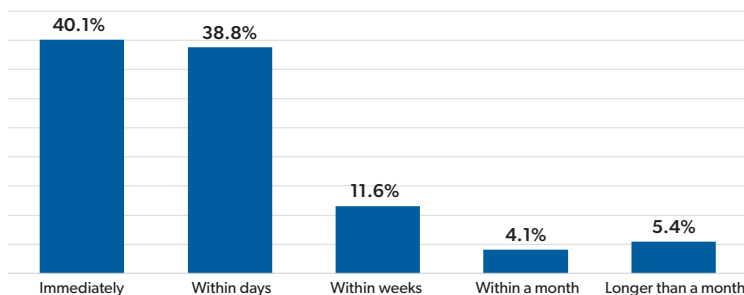


Figure 10. Typical Length of Time Required to Discover Check Fraud

Once fraud is committed, how likely is it that the stolen funds are recovered? As seen in Figure 11, nearly two-thirds of respondents reported retrieving between 75 and 100 percent of the money. While that's good news, identifying the issue and taking action to recover the funds is time-consuming, so it comes with an unseen cost. A full 10 percent of survey participants were able to recover half or less of the stolen funds, and six percent were unable to recover anything.

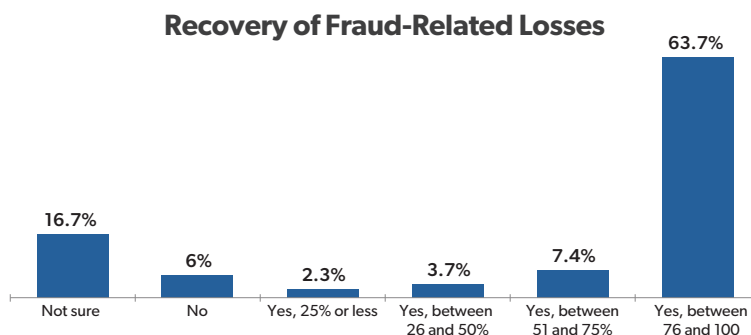


Figure 11. Successful Recovery of Fraud-Related Losses

Segregation of Duties

An important best practice for accounts payable teams is segregation of duties, or SOD. IOFM has many resources that detail the importance of preventing a single individual from having too much control of company funds because it's an invitation to internal fraud. (See Control Fundamentals: Segregation of Duties for more information.) However, this can be difficult to implement in small organizations with limited staff.

Do survey participants have SOD policies in place? Figure 12 shows that most do. However, over 10 percent either don't employ a segregation of duties policy or don't consistently enforce it. That is an invitation to fraud perpetrated by unscrupulous employees.

Establishment and Enforcement of Segregation of Duties (SOD)

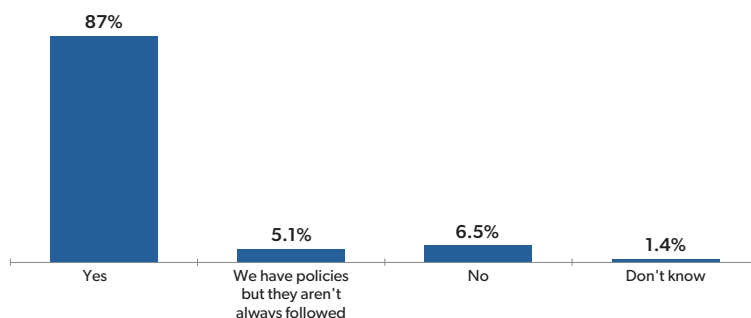


Figure 12. Enforcement of Segregation of Duties Policies

Let's take a look at how that plays out in terms of fraud attempts. Regardless of SOD policies, fraud was up across the board in 2024, as seen in Figure 13. However, those organizations with no segregation of duties policies in place saw a 57 percent increase in fraud attempts in 2024 vs. 2023, outpacing companies with these policies, even if they weren't able to consistently implement them. This trend is likely to continue, given the economic challenges we are beginning to experience in 2025, and will probably lead to more instances of internal fraud.

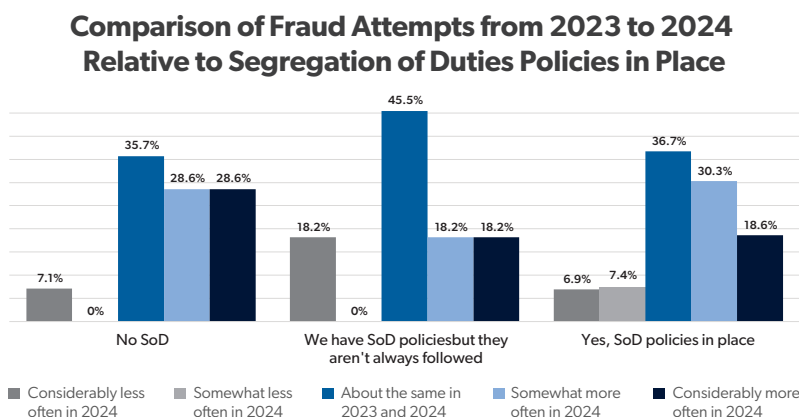


Figure 13. Frequency of Fraud Attempts Based on Segregation of Duties Policies, 2023 vs. 2024

Once fraud has been attempted, how long does it typically take an organization to identify that it's been targeted? Here, segregation of duties compliance makes a significant difference in the length of time required to discover fraud activity. Figure 14 shows that those companies who rigorously enforce SOD detected nearly half of attempts immediately, and over a third of the remaining frauds within just a few days. It typically took those organizations who have policies but don't always follow them a few days longer to discover the fraud attempts, but more than a third of departments without any SOD whatsoever took weeks or even months to detect them.

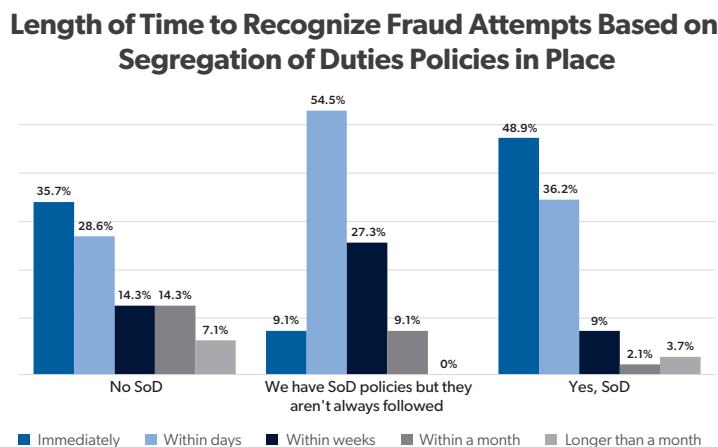


Figure 14. Time Needed to Recognize Fraud Based on Segregation of Duties Compliance

That's noteworthy, because when it comes to fraud, time is of the essence.

The Role of Automation

With fraud on the rise, detection software can play a significant role in protecting an organization's funds. Expecting staff to detect fraudulent activity while performing their regular AP responsibilities is asking a lot, and a technique that's haphazard at best. But what tactics do software solutions use to thwart fraudsters?

Campbell explains, "Fraud detection software significantly reduces the number of fraud instances primarily through real-time monitoring of transactions and activities. Behind the scenes, the software performs several tasks, including:

1. Comparing known data elements of an individual, entity, device or location with newly entered data;
2. Analyzing transaction patterns, vendor names and identifiers, and purchase dates and amounts;
3. Generating alerts for human review of anomalies or "out of policy" activities.

With the integration of AI capabilities, the software can learn from historical data to adapt to evolving fraud schemes. This continuous learning enhances accuracy and improves the detection of new fraud methods."

Yet, most organizations don't use this valuable fraud-busting tool, as Figure 15 shows. More than half of companies polled don't have it, while just a third do.

Organizations Employing Software for Fraud Detection Purposes

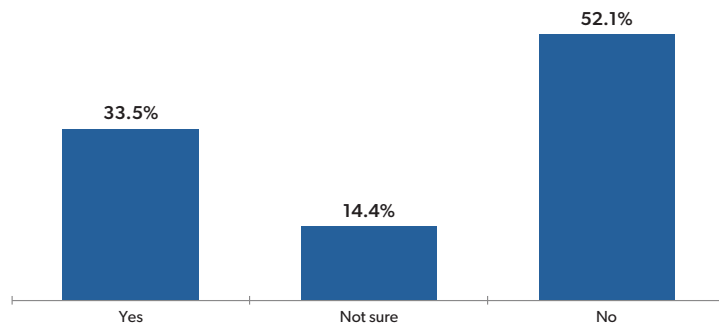


Figure 15. Percentage of Organizations Using Fraud Detection Software

Figure 16 clearly shows that those organizations who do use fraud detection software are significantly less likely to become targeted by fraudsters.

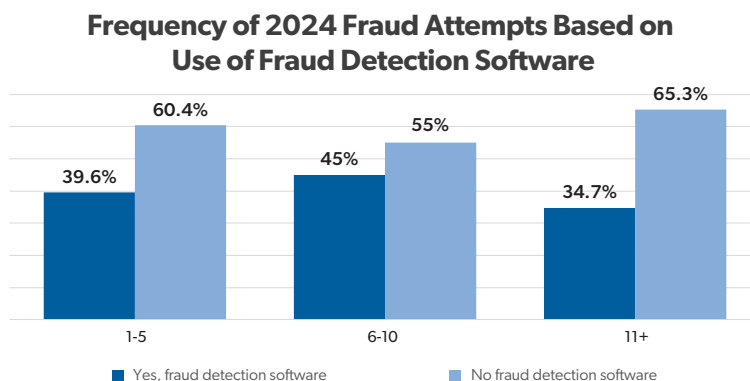


Figure 16. Impact of Detection Software on Fraud Attempts

Fraud on the Rise

The takeaways are clear.

Fraud is on the increase, and is expected to continue to grow. This is driven by global financial stress; the rapid evolution of fraud techniques such as AI that make it easier to trick AP professionals into making fraudulent payments; the lack of internal controls such as segregation of duties; the continuing use of paper checks; and reliance on staff to catch fraud activity instead of using automation tailored to the job.

Campbell offers this advice: “Finance professionals must remain vigilant. Here’s what I recommend. Stay informed about emerging fraud schemes. Advocate for robust internal validation processes for bank information, tax details, email addresses and shipping addresses. If your validation process is manual, ensure it includes checks and balances, and relies on trustworthy sources.”

Ultimately, however, as fraudsters get increasingly clever at using technology to trick AP staff, she concludes it’s best to fight fire with fire. She says, “Investing in technology is the best strategy to safeguard the organization while also delivering excellent service.”

About Esker

Esker is a global cloud platform built to unlock strategic value for finance and customer service professionals, and strengthen collaboration between companies by automating the cash conversion cycle. Esker's solutions incorporate Artificial Intelligence (AI) technology to drive increased productivity, enhanced visibility, reduced fraud risk, and improved collaboration with customers, suppliers and internally. Esker operates in North America, Latin America, Europe and Asia Pacific with global headquarters in Lyon, France, and US headquarters in Madison, Wisconsin. In 2020, Esker generated 112 million euros in total sales revenue.

For more information, visit esker.com



About the Institute of Finance & Management

Accounting and finance professions have each undergone nothing short of a complete transformation since the Institute of Finance and Management (IOFM) was founded in 1982 and since then our mission has been, and continues to be, to align the resources, events, certifications, and networking opportunities we offer with what companies need from the accounting and finance functions to deliver market leadership. IOFM empowers accounting and finance professionals to maximize the strategic value they offer their employers.

Our enduring commitment to serving the accounting and finance professions is unmatched. IOFM has certified over 25,000 accounting and finance professionals and serves several thousand conference and webinar attendees each year.

IOFM is proud to be recognized as the leading organization in providing training, education and certification programs specifically for professionals in accounts payable, procure-to-pay, accounts receivable and order-to-cash, as well as key tax and compliance resources for global and shared services professionals, controllers, and their finance and administration (F&A) teams.

Learn more at [IOFM.com](https://iofm.com)