organizations need to place a heavier reliance on technology. AP teams armed with powerful and intelligent AP automation technology can do more than win a battle against fraud.

Apr. 19, 2022

Fraud is as old as commerce itself. You might think that by now organizations have figured out how to battle back against fraud and prevent it from hurting their business operations and reputation. Unfortunately, the opposite seems to be occurring. Just as business processes have become more sophisticated over the course

of time, so too has fraud matured. In fact, fraudulent activity seems to be

making it the most prevalent type of BEC attack.

Financial institutions in particular are on high alert when it comes to fraudulent activity. The threat of regulatory non-compliance looms large for finance organizations, and with the customer life cycle undergoing dramatic transformation, it may seem more challenging than ever to protect the business.

No one wants to be the victim of fraud, but history has proven even the world's biggest companies aren't immune to financial deception. Take Google and Facebook, for example. In 2019, both companies were scammed out of more than $100 million due to phishing emails containing forged invoices. The emails were sent to the accounts payable department, and even though both companies had certain security measures in place, the seemingly legitimate invoices were processed. Then there's the story of American tech entrepreneur Mark Cuban, who had $82,000 stolen from his first company by an employee cashing fake checks at the bank. The lesson here is any company is vulnerable to fraud when the right safeguards aren't in place.

So what are the proper measures? The key to preventing fraud—and fulfilling "know your customer" (KYC) requirements—is the right mix of people, processes and technology. But as fraud has become more sophisticated and the landscape is constantly changing, success demands organizations, especially AP teams, place a greater reliance on the technology piece of the fraud detection puzzle. People will always play a role, but as scammers get harder to identify, it becomes more difficult for humans to weed them out. Processes also have a part in fraud mitigation, but they must be crafted in ways that unite people and technology.

Which brings us to the tech component of the fraud protection equation. Technology, just like fraud, has become more advanced, so it can accomplish things even the best people and processes can't. It's the strongest defense against

increasingly sophisticated fraudsters, and it's the one element most resistant to

percent of AP teams support fraud prevention and compliance activities."

Since fraud is evolving and scammers are becoming more sophisticated (and dangerous) in their tactics, AP staff need to modernize their approach. Intelligent AP automation is a smart investment for financial organizations looking to bolster their defenses. Automation delivers direct benefits to the people, processes and technology responsible for stopping fraudulent activity.

The Ardent report specifically discusses the benefit of automation, stating, "As a byproduct of transforming itself, AP can better support compliance and risk management teams in enforcing policies, identifying potential red flags and escalating issues internally." Eliminating error-prone manual work is at the heart of this transformation. An AP automation solution establishes standards for handling exceptions and workflows, which reduces the fraud risk and increases compliance.

Australian businesses in particular are starting to realize the importance of technology in fraud prevention, with 38 percent reporting using forensic data analytics or artificial intelligence to help detect fraud and corruption in the KPMG survey. But how, exactly, does AP automation help stop fraud in its tracks?

AP Automation: The Technology Leading the Charge Against Fraud

There are several intelligent AP automation technologies that work together to shield finance organizations from fraudulent activity:

- *AP automation solutions* (APA) automate invoice processing, saving time and reducing errors.
- *Process orchestration* automatically routes exceptions for human review and approval and maintains a trail of handoff between human and digital workers.
- *Artificial intelligence* determines the invoice layout and identifies the right information needed, regardless of format.

- *Multi-channel invoice capture* automates the process no matter how suppliers

Properly armed with the right technology, AP teams can fight back against fraud in many ways:

- Automation eliminates the errors associated with manual invoice processing, which can result in duplicate payments or the approval of fraudulent invoices.
- Automation can flag the submission of fake invoices coming from unknown vendors.
- Purchase order matching ensures invoices are for the exact goods ordered or received.
- Approval and exception workflows can be automatically triggered for invoices over a certain amount, coming in from a new vendor or if the amount doesn't match the PO.
- Freed from manual invoice processing, AP staff can focus on exceptions and apply their knowledge to unusual changes in vendor behavior.
- Advanced analytics enable the AP team to note trends in vendor behaviors and identify changes that may warrant investigation.
- Audit trails provide the data needed to track down potentially fraudulent activities.
- Verification from third-party sources helps prevent identity fraud among new suppliers and vendors during the onboarding process.

It's the combination of people, processes and technology which ultimately safeguards a company's cash. As fraud has evolved and become more difficult for humans to identify, finance organizations need to place a heavier reliance on technology. AP teams armed with powerful and intelligent AP automation technology can do more than win a battle against fraud—they can win the war. From simple employee forgeries to complex cyber threats, intelligent automation is leading the charge against fraud and helping AP teams work like tomorrow, today.

========

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us