Best Practices to Fight Fraud With AP Automation

BY MICAH REMLEY

Criminals are like rivers—they flow where there is the least resistance. They seek out the areas where they can get the biggest return on their time, always uncovering the easiest vulnerabilities that open the door to large payouts.

Over the years, criminals have learned that it has become very difficult to trick banks into initiating a fraudulent transaction. Instead, they target companies. And, which is the most vulnerable department inside a company? The accounts payable (AP) department that handles large business-to-business (B2B) payments to multiple vendors at a time.

Many businesses mistakenly believe they are most vulnerable to accepting fraudulent payments. However, with the rapid uptick in sophisticated fraud from all fronts, companies need to be prepared for fraud from anywhere—especially the AP department.

Unfortunately, these fraud attempts are getting more pervasive. According to the Association for Financial Professionals (AFP), 78% of businesses were impacted by payments fraud last year, continuing a five-year trend of increased fraud exposure. What's more, businesses are facing a continuous threat of fraud coming from "traditional" operational tasks, such as paper-based or manual processes. For example, in a recent AFP survey, 70% of organizations cited being exposed to check fraud in 2018. Most recently, a subsidiary of automaker Toyota was scammed out of more than $37 million in fraudulent vendor invoices.

Criminals rely on the manual and complex processes for AP account set-up to create vulnerabilities in businesses of all sizes. AP managers are often responsible for tracking down the vendor's tax identification numbers, verifying the

company's physical location, and more—all while manually keying in or filing this information. This leaves significant room for error, such as the following:

- Supplier onboarding without proper vetting
- Reliance on paper checks, which are the riskiest payment method
- Fictitious invoice creation
- Duplicate vendor payments

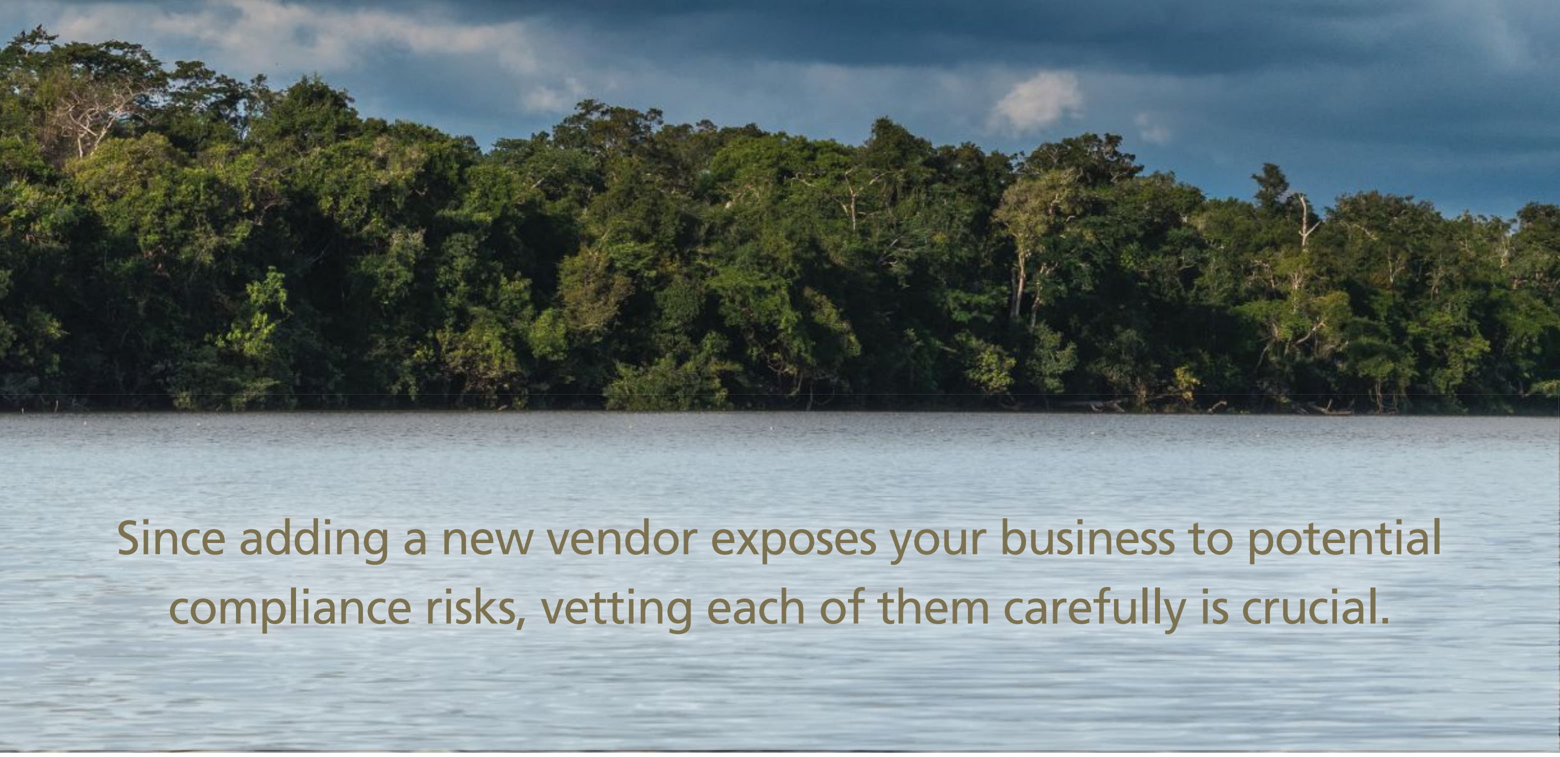
Here are a few simple best practices that any AP department, large or small, can implement to effectively mitigate fraud risk related to vendor payments.

Properly Vet Your Suppliers

Since adding a new vendor exposes your business to potential compliance risks, vetting each of them carefully is crucial. A well-rounded approach to vetting new vendors includes the following steps:

- **Ask the right questions**—This may involve asking detailed questions to the vendor or doing research outside of discussions. Before onboarding any new vendors, ask these questions:
  - How long has the company been in business?
  - Has it changed locations frequently?
  - How many employees does the company have?
  - What is the company's revenue?
- **Look for red flags**—Don't ignore even the smallest red flag. Some of the most common warning signs of potential fraud include high employee turnover or a low Better Business Bureau rating. If the vendor is cagy about answering some of the questions previously mentioned, you should see that as a red flag. Finally, if you're requested to send a payment indirectly to the company, such as mailing it to a residential address instead of the company's official address, you should pay close attention to that warning sign.

Micah Remley is President and Chief Executive Officer (CEO) of MineralTree. As CEO, Remley leads the company strategically, both internally and externally, developing new success strategies and ensuring growth and development.



Since adding a new vendor exposes your business to potential compliance risks, vetting each of them carefully is crucial.

- **Be aware of positive signs**—Onboarding a vendor should comprise balancing the negatives and positives. Look for good signs, such as transparency during the vetting process and the ability to answer and provide specific details about processes. Determine if it is a growing business or one with longevity and a strong reputation.

Manage Vendor Risk Long Term

Some might be thinking, "We always properly vet our vendors when we onboard them. Isn't that the end of the vetting process?" The short answer is no, especially if the AP department is relying on outdated, manual processes and paper checks. In order to protect the business from AP fraud on a consistent basis, companies should think about all of these as good best practices.

Transition to Electronic Payments

Electronic payments mitigate fraud and increase efficiency. For example, ACH transfers add layers of security by encrypting data but may take one to three days to transfer. Additionally, not all companies are enabled to make ACH payments through their banks due to the underwriting process. Instead of relying on traditional methods, consider adopting the use of virtual cards that have tokenization capabilities. These one-time-use cards add a layer of protection by never using the same card number twice. Additionally, virtual cards often have a loyalty component associated with them. This means every vendor payment can earn rewards for the business.

Employ Segregation of Duties

Why give one individual full autonomy over the payments process? Set up a process that has distinct duties for managers, approvers, and authorizers to ensure that payments are processed correctly. Particularly in smaller businesses, this may seem impossible, but having checks and balances integrated into the AP process can protect your business from fraud while saving time and money long term.

Automate Your AP Process

An AP automation solution can help combat fraud by embedding payment controls, such as segregation of duties, into the AP process. Examples of how an AP automation solution can streamline and protect the business include the following:

- **Dual-factor authentication**—Dual-factor authentication adds another layer of security by requiring employees to enter a unique security code that they receive via text or email every time they release funds
- **Auto PO matching**—If your company's AP process includes purchase orders, an automated solution can match corresponding invoices automatically and flag any that are mismatched
- **Positive pay files**—Many AP automation systems employ the use of positive pay files, which are automated fraud detection tools that transmit a file of all issued checks to corresponding banks each day, enabling them to verify that every check payment is authorized

Putting an automated AP process in place can easily protect your business, especially as new vendors are added into the system.

The process companies put in place for vendor management can provide unparalleled security for the company now and in the future. In order to best protect the company from fraud, ensure the process consists of thorough vetting at the beginning. Most importantly, this vetting will incorporate controls that can identify red flags throughout the relationship. Consider using automation as a tool to help supplement AP management to easily monitor where vendor payments are really going to further protect the business. And remember: No company is too small or large to properly vet. ■