Disarming Risk

In Procure to Pay

Safeguarding your AP Process

Oversight

The Accounts Payable (AP) process is a value driver.

64% of all business executives – up from 60% in 2020 – believe their AP team is either "very valuable" or "exceptionally valuable" to their business stakeholders and suppliers, according to Ardent Partners' study, Accounts Payable Metrics that Matter in 2024.

The global pandemic may have kept employees home, but the AP process never skipped a beat.
Business continuity was a primary concern when companies were forced to close their offices to all but essential staff. While bills continued to roll in, AP teams stepped up to ensure timely payments were made, once again proving their value.

There is much more to accounts payable than just data entry and payment. Between vendor master set-up, purchase orders, invoice entry, and payment, there is a great deal of responsibility put on AP teams. Multiple spend channels and disjointed systems provide siloed views of spend data, making it difficult to manage financial and compliance risks.

Such internal challenges are compounded by increasing external threats. Scammers are eager to capitalize on gaps in organizational controls and payment systems to defraud companies out of millions of dollars, all the while tarnishing their reputations with customers and stakeholders. With a purpose-built technology solution, organizations can quickly scan large volumes of data from multiple source systems to identify, prioritize, and mitigate otherwise undetectable risks. Utilizing technology can improve the effectiveness of their AP processes.

How financial leaders are tackling AP risk today.
The highest-performing finance teams in the Fortune 500 are deploying AI-powered technology to improve controls and reduce fraud, error, misconduct, and noncompliance. Why?

Because AP risk can come from multiple vectors, and only AI-powered platforms can detect all this risk at once, automatically. Risks that include:

- Duplicate Payments
- Vendor Master Integrity
- Fraud Schemes
- Undetected Losses

Duplicate Payments

Duplicate invoice payments occur far more often than most realize, resulting in unnecessary cash leakage.

Data from APQC's Open Standards Benchmarking® Accounts Payable survey indicates that companies make duplicate or erroneous payments at a rate of 0.8% to 2%. While these numbers seem insignificant, they reflect the percentage of disbursements and not the amounts of the disbursements themselves. So, even one duplicate entry could put a serious dent in your cash reserves.

Most organizations depend on their ERP systems and internal controls to prevent duplicate payment errors. However, even with manual approval processes, SOX control testing, and data sampling , cash leakage continues.

Although simple data entry errors are the primary cause of duplicate payments, there are other reasons for their occurrence:

- Vendor sends multiple invoices to different individuals
- Paying by invoice and by statement
- Duplicate vendor records exist
- Vendor is paid using P-Card while AP pays the invoice for the same purchase

It is unreasonable to think approvers will capture every error during the review process. It is also unrealistic and inefficient to require internal audit and AP departments to sift through invoices manually to look for potential duplicate entries.

Controlling duplicate invoice payments becomes even more difficult in cases involving numerous invoice-receiving methods and locations, various payment methods, and less than pristine vendor master records.

Vendor Master Integrity

If you tried to maintain an Excel spreadsheet listing every supplier you've ever done business with, you would probably wind up with a list that has a few mistakes in it. Vendor master errors, particularly duplicate records, pose risks you might never have considered:

Limited Spend Visibility

If you spread the purchases from a vendor across multiple records, it becomes harder for your organization to gain a complete view of what has been spent with that entity. Imagine sitting down to negotiate future pricing with a vendor based on limited data that reflects spend totaling in the hundreds of thousands when the amount is actually in the millions. Incomplete information limits negotiating power.

Duplicate Payments

When there are duplicate records for a vendor, you may issue payment twice to that vendor, creating the same visibility issues as above.

Internal Fraud

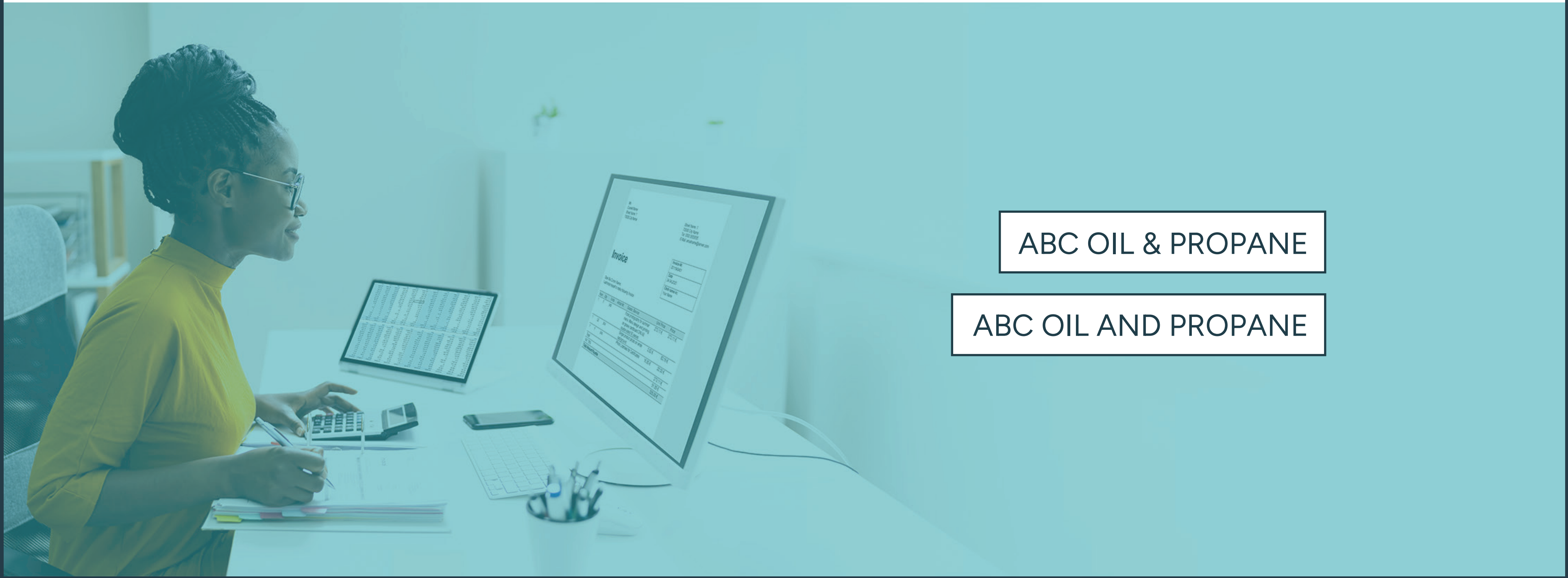
When the vendor master contains errors, it opens the door to fraud. Let's say our fraudster accesses the vendor master and creates a duplicate listing with new banking information. If organizations don't check for duplicate listings, they could be sending money to fraudsters for months or even years before realizing it.

External Fraud

In March of 2019, a Lithuanian man pleaded guilty to defrauding a couple of companies out of more than $100 million. How did he do it? By taking advantage of the uncertainty created by duplicate listings in the vendor master, he was able to successfully breach the vendor master, posing as a supplier. When he submitted invoices, they were paid without question. $100 million dollars in fraudulent payments were disbursed before the issue was noticed.

Delayed Payments

Most payment delays are the result of human error. Data entry errors such as entering the wrong street address, PO Box number, or zip code at the vendor master level or selecting the wrong vendor when there are multiple accounts can lead to untimely payments and late charges. Delayed payments can also open the door to supply problems or the loss of services.



ABC OIL & PROPANE

ABC OIL AND PROPANE

Fraud Schemes

In 2024, 62% of invoices were paid electronically, per Accounts Payable Metrics that Matter.

The past couple of years have only reminded us of the dangers and challenges of relying on paper checks and manual processes. And while electronic payment methods continue to offer greater efficiency and more security than paper checks, fraudsters continue to successfully infiltrate electronic payments through schemes such as business email compromise (BEC) and vendor impersonation.

In 2023, checks and ACH debits were reportedly the payment methods most impacted by payment fraud activity. While check fraud remained stable at around 65% from 2020 to 2023, ACH payment fraud increased, rising from 34% in 2022 to 47% in 2023.

With better training, policies, and procedures, companies have become better at detecting and mitigating BEC. Down by eight percentage points from 2020, only 63% of organizations were targeted by BEC in 2023.

Emails from fraudsters impersonating vendors, third parties requesting bank changes, and fraudsters posing as senior executives requesting fund transfers are the most common types of BEC attacks companies are falling victim to.

63% of organizations experienced BEC in 2023

Undetected Losses

One common misconception with AP recovery is the notion that "what was recovered is what was lost." This is not always the case for businesses that lack visibility into their total spend risk.

There are many additional ways that smaller risks compound into more significant cash leakage:

High Turnover and Limited Training

Some organizations report lower productivity, diffused organizational culture, and diminishing quality of work due to less experienced employees and high turnover in processing staff. These can affect the output, costs, and other corporate considerations that impact the bottom line.

Dependence on ERPs and Other System Controls

Organizations deploy ERPs and AP automation platforms with the hope of creating process efficiencies and improving controls. In actuality, this often just shifts work to other areas of the business, such as IT, which may be depended on to produce reports from the ERP. It becomes a time consuming endeavor for IT and can also generate many false positives that ultimately diminish the productivity of the AP team.

To fully understand the source of cash leakage, fraud, and misuse, an organization's AP audit process needs to go beyond sampling and manual attempts to monitor transactions across disparate source systems. Organizations should move from disjointed, laborious auditing processes toward automated, continuous monitoring and analysis that flags anomalies and initiates further investigation before payment occurs.

AI and the Power of Prevention

As organizations work to digitally transform their finance functions, many deliver greater business value by adopting AI-powered technology. Automation allows more time to analyze data, stave off threats posed by fraud, and prevent misuse and abuse of company funds in advance.

There is a goldmine of data in AP, and it can be used to deliver protection from fraud, misuse, and waste by watching patterns and learning from inputs with AI. In fact, organizations using data monitoring or analysis detect fraud 56% faster.[1]

And still, 36% of organizations have yet to implement an automated AP spend management solution.[2] The mission remains to educate leaders on the value.

Oversight has helped the world's most innovative companies and government agencies digitally transform their spend audit and financial control processes. So if you're looking for an AI-based spend management and risk mitigation solution, you've come to the right place.

[1] ACFE 2022 Report to the Nations
[2] Ardent Partners Accounts Payable Metrics that Matter in 2022

Organizations using data monitoring or analysis detect fraud **56%** faster.

How Oversight Provides Ongoing Protection

Leading organizations are deploying Oversight's solution for AP to continuously monitor transactions for errors and outlier activities that could indicate fraud and misuse.

Oversight uses AI to detect and resolve issues by:

1 Finding Invoice Numbers That Closely Match

Fuzzy matching is a more powerful method for detecting duplicates than exact matching. Similarity analysis is applied to invoice numbers to identify keying errors such as transpositions or additional or missing characters..

2 Pinpointing Cross-program Duplicate Payments

Automatically compare AP data to expenses and purchase card transactions with multiple solutions in place, allowing for the detection of cross-program duplicate payments as well as recurring employee or vendor involvement.

3 Detecting Duplicate Vendors

Duplicates are identified using data attributes such as similarity of company names and addresses. The presence of duplicate vendors in the vendor master is one of the top causes of duplicate payments.

4 Identifying Outliers

Outliers could include invoice amounts that are higher than the vendor's average, an increase in the volume of invoices, or invoices with rounded amounts, all of which are common tactics used by fraudsters.

5

Flagging Out-of-Norm Entries

When an invoice payment is made on the weekend or a holiday, further investigation is typically warranted. By flagging unusual invoice entries and off-cycle payments, issues are brought to the forefront quickly.

6

Catching Incomplete Information

Advanced technology automatically identifies missing or incomplete vendor data and flags vendors with invalid or suspicious addresses. Correcting missing information can be the easiest way to cut risk within your vendor master, but it also pays to look for employee-vendor relationships, sudden changes in vendor banking or payment details, and potentially fictitious vendors.

7

Highlighting Inefficiencies

By isolating the root causes of errors, organizations can focus on strengthening controls and processes. Better visibility into AP data helps companies detect duplicate and erroneous payments, fraud, and misuse to prevent unnecessary cash leakage. Better yet, the right tool will not only enable the prevention of errors in the first place, but will also efficiently analyze data across multiple payment platforms while providing a case management system to build robust audit trails.

8

Identifying Risky Vendors

Vendors are assessed based on information such as their business address and evaluated against national, global, and government watch lists to ensure compliance with regulatory requirements.

Gain Visibility Into Your Full Spend Risk

ERP and AP Automation platforms are not effective audit controls. To successfully manage spend risk, you need a system with advanced technology that is purpose-built to monitor the gaps in your controls. Today, finance leaders have a tremendous opportunity to transform audit and risk management processes.

Oversight's spend management platform enables your organization to identify spend risk no matter where it resides. Our AI-powered platform looks across spend categories–Accounts Payable, Travel & Expense, and P-card–to identify and prioritize risks, allowing you to take immediate action to mitigate those risks.

Oversight's AI-driven insights eliminate the need for manual, sample-based audits, performing right-time analysis on every invoice, every payment, and every vendor to identify unusual spend patterns, data entry inconsistencies, and improper purchasing activities. With full visibility into spend risk, Oversight allows you to take a proactive approach to spend risk mitigation, preventing mistakes before payment happens.

Oversight safeguards your spend, so you can proactively disarm the risks facing your Accounts Payable processes.