REPORT

The Rise in AP Fraud – Frequency, Sophistication, and Impact

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.

Sponsored by basware Now it all just happens™

Written by sharedserviceslink

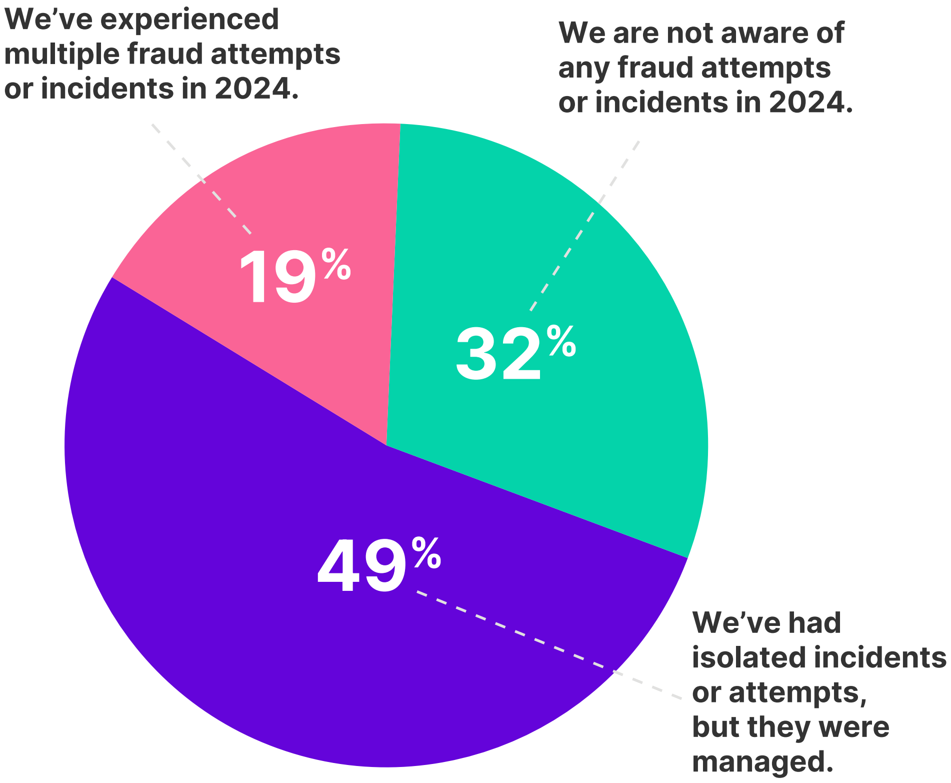
Introduction

Accounts Payable (AP) fraud is surging in frequency and sophistication, with increasing numbers of organizations being targeted each year. In this report, we will share how companies are feeling overwhelmed by the threat of fraudulent attacks and unsure as to how to resolve the issue.

Our findings show that **68% of organizations encountered at least one fraud attempt in 2024.** 19% experienced multiple attempts, with the other 49% facing isolated incidents.

The minority of respondents (32%) say they are unaware of any fraud attempts made on their business. However, this doesn't rule out possible occurrences of fraud—they may have gone undetected.

How would you rate your organization's current exposure to AP fraud risks?



This concerning trend mirrors broader industry findings, with the Association for Financial Professionals (AFP) reporting that **80% of organizations were targets of payments fraud in 2023**, a 15-percentage-point increase from 2022[1].

[1] 2024 AFP Payments Fraud and Control Survey Report

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.

Sponsored by basware Now it all just happens™

Written by sharedserviceslink

Growing Consensus: AP Fraud is Worsening

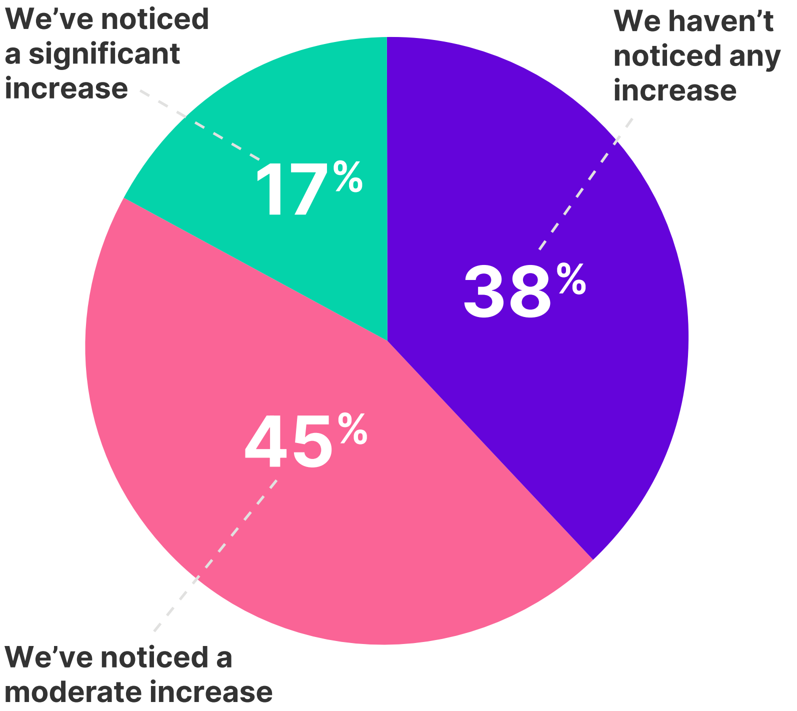
The majority of our survey respondents recognize the growing challenge, with **62% stating that fraud attempts have worsened over the past year.** While 38% say they haven't noticed an increase, it also may not be a metric that is reviewed regularly.

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.

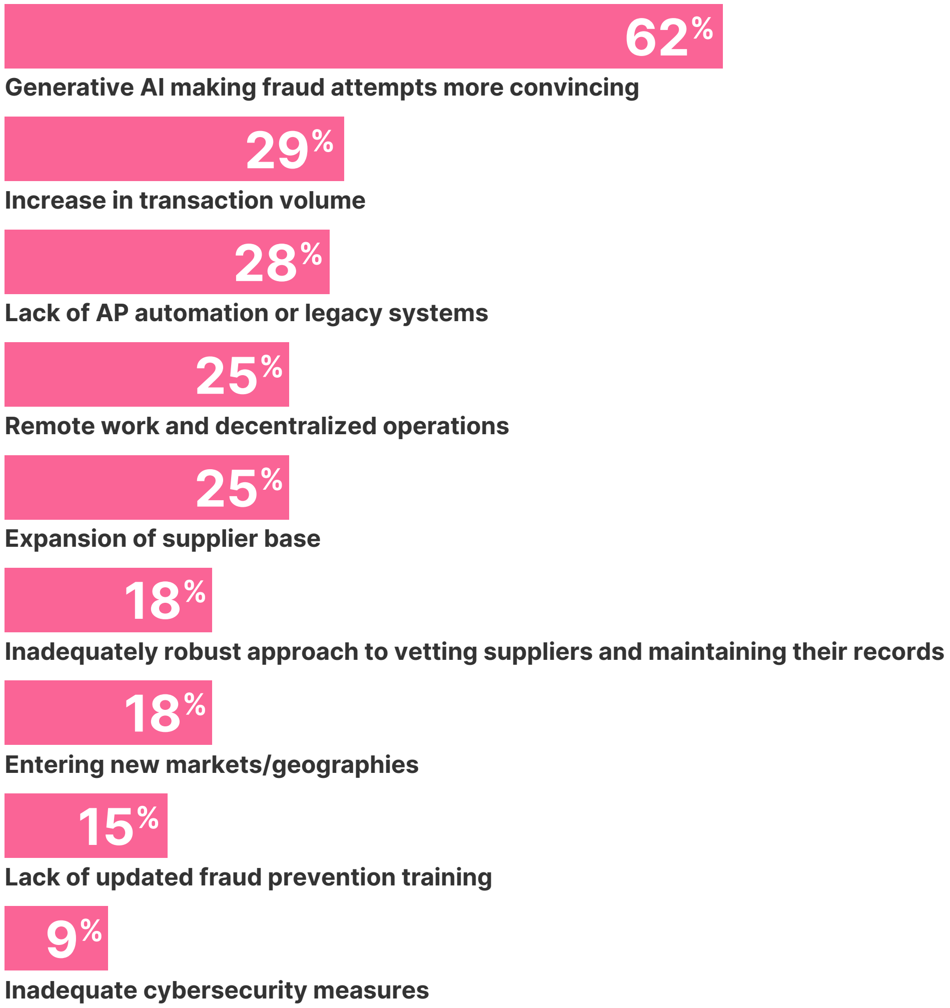
Sponsored by basware Now it all just happens™

Written by sharedserviceslink

Do you think your organization's exposure to AP risk or fraud has increased in the last 12-24 months?



Here is a list of key factors contributing to increased fraud in AP today:



Key Drivers of Rising AP Fraud

Several factors contribute to the rise of AP fraud. Our survey highlights both technological and operational changes that are making fraud easier to attempt, and harder to detect.

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.

Let's Look at the Top Four:

1. **Generative AI Makes Fraud Attempts More Convincing:** One of the most significant factors driving AP fraud today is the role of Generative AI in creating convincing materials that aid fraudulent activity. 62% of our respondents identified Generative AI as a primary contributor to the increase in fraud. The accessibility of this technology has increased dramatically in the last two years. AI can be used to produce highly authentic-looking documents and emails, and even voice impersonations that mimic suppliers or executives, enabling fraudsters to deceive AP departments. As GenAI attempts increase both in volume and sophistication, it's harder to distinguish legitimate communications from fraudulent ones.

2. **Lack of AP Automation (28%):** Human eyes and traditional tools are not able to keep up with auditing the sheer volume of complex transactions in large organizations. Manual processes are time-consuming and prone to human error, making it difficult to accurately match invoices, track approvals, or identify duplicate payments. The absence of real-time monitoring means that unusual patterns or potential fraud can go undetected for weeks—or even months—until they cause significant financial damage. For overworked and understaffed teams, these challenges are compounded, leading to bottlenecks in invoice approvals, missed payment deadlines, and strained supplier relationships. AP automation is key not only to improving efficiency, but also tackling security risks and operating effectively and compliantly.

3. **Increased Transaction Volume and Supplier Base:** Roughly a quarter of respondents point to an increase in transaction volume (29%) and expansion of the supplier base (25%) as critical risk factors. AP teams must handle a greater number of invoices and communications, often under tight deadlines while juggling various other time-pressing demands. This expanded workload is unscalable without technological support, and it creates blind spots and a willingness to shortcut manual process. AP automation enables teams to process high volumes of transactions efficiently, track supplier interactions at scale, and reduce risk and errors with built-in controls and real-time analytics.

4. **Remote Work and Decentralized Operations:** 25% of respondents cite remote work and decentralized operations as contributing factors to increased fraud risk. The lack of physical oversight and reliance on digital processes that comes with remote work can make it easier for individuals to manipulate invoices, create fictitious vendors, or approve unauthorized payments. Decentralized operations can further complicate the detection of such fraud, with the dispersion of responsibilities and lack of centralized monitoring leading to delays in identifying and addressing discrepancies. This environment necessitates robust digital controls and vigilant monitoring to mitigate the heightened fraud risk.

What Does AP Fraud Look Like?

- **Internal fraud** from employees.
- **External fraud** with tactics like invoice cloning, unauthorized changes to bank account information, and other external manipulation.
- **Collaborative Fraud:** Weak controls and limited visibility into the invoice process can open the door to fraudulent schemes involving collusion between employees and third parties. These schemes often exploit gaps such as poor segregation of duties or lack of oversight, enabling kickbacks, falsified invoices, or duplicate payments to go unnoticed. Without robust controls and transparency, organizations risk enabling intentional collaboration to defraud the company, often under the guise of legitimate transactions.
- **Non-malicious fraud:** Mistakes from manual handling, overpayments, or duplicate payments that can result in financial losses.

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.

Sponsored by basware Now it all just happens™

Written by sharedserviceslink

Challenges Facing AP Departments: Contributing Factors to Rising Fraud Risk

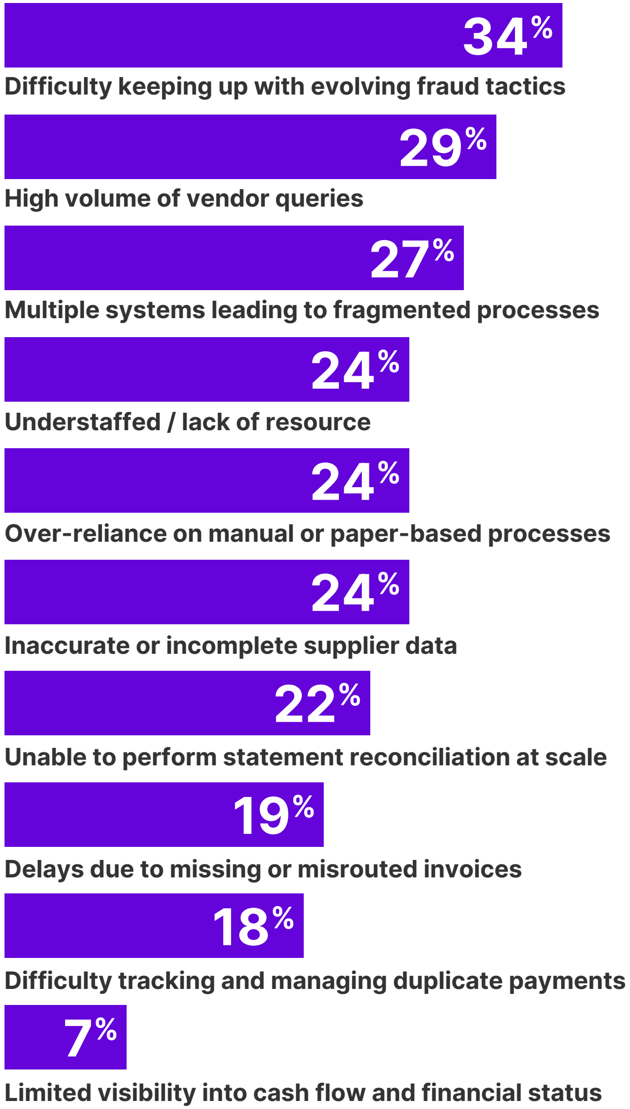
AP teams are on the front line of managing payments and spotting fraud, but a "firefighting," reactive culture in AP means that having a proactive and preventative attitude towards fraud becomes less of a priority.

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.

Sponsored by basware Now it all just happens™

Written by sharedserviceslink

Common challenges in AP today:



Looking at the top five issues, you can see clear contributing factors in the failure to prevent fraud:

1. **Adapting to Evolving Fraud Tactics (34%)**
   Fraud techniques are evolving rapidly, with Generative AI and sophisticated phishing methods adding complexity.
2. **High Volume of Vendor Queries (29%)**
   When inundated with vendor inquiries, AP teams don't have the time to scrutinize each communication or dispute closely. Some vendors are also using automated methods to raise disputes (both legitimate and illegitimate), which dramatically increases the volume of messages hitting AP's inbox.
3. **Fragmented Processes Across Systems (27%)**
   Multiple systems can lead to inconsistent controls and create data silos. When platforms don't communicate seamlessly, it is harder to identify fraudulent transactions across the AP process.
4. **Limited Resources and Staffing (24%)**
   With AP teams' stretched workloads, there is often little time for thorough transaction reviews. As workloads increase, priority may be given to processing payments to hit KPIs, over double-checking authenticity.
5. **Reliance on Paper-Based Processes and Limited Statement Reconciliation (24% and 22%)**
   The reliance on paper-based processes and the inability to reconcile supplier statements at scale creates significant blind spots in AP operations. These gaps make it challenging to verify the authenticity of invoices, detect duplicates, and ensure accurate payment records. Without a unified solution that can process invoices and perform large-scale statement reconciliation, AP teams are left vulnerable to errors, fraud, and inefficiencies.

From manual processes and limited visibility to high transaction volumes and inadequate resources, each challenge contributes to exposure to increasingly complex fraud tactics. **Addressing these issues will require investment in digital tools, streamlined processes, and fraud-focused training, to help AP departments stay resilient against this rising threat.**

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.

Management of Fraud Prevention Efforts in AP Departments

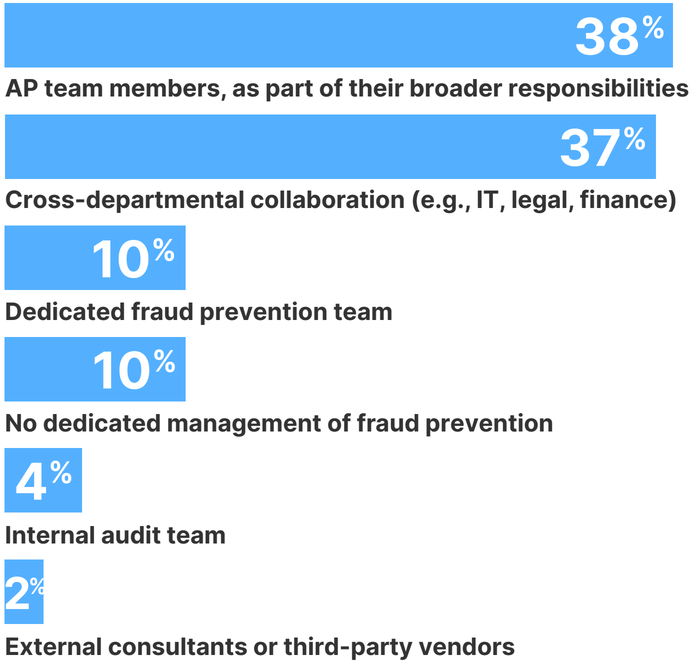
Respondents shared different approaches to fraud prevention, highlighting a mix of dedicated roles, shared responsibilities, and cross-departmental collaboration. Having an integrated approach is common–only 10% say they have a dedicated fraud prevention team for their AP department.

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.

Sponsored by basware Now it all just happens™

Written by sharedserviceslink

Who primarily manages fraud prevention efforts in your organization's AP department?



- The most commonly-cited response (38%) stressed a reliance on **AP team members to handle fraud prevention as part of their broader responsibilities**. This approach can lead to challenges, as AP staff may be stretched with their regular tasks, and may lack the specialized skills, knowledge, experience, or resources necessary to thoroughly address fraud risks.
- Just over one-third of organizations (37%) approach fraud prevention through **cross-departmental collaboration**, involving IT, legal, and finance. This collaborative model enables AP departments to share and access expertise from different functions, widening the brain power to combat fraud. But managing multiple stakeholders can also lead to slower response times and coordination challenges if roles and responsibilities are not clearly defined. Effective cross-departmental collaboration is only possible when you have the fraud detection tools in place to provide accurate information that can be seen across departments.
- Only 10% say they have a **dedicated fraud prevention team**. Such a team is ideal to help shield against the ever-evolving threats of fraudulent activities across all departments.
- 10% of respondents reported **no dedicated fraud prevention management** in their AP department. This lack of structured oversight could make these organizations particularly vulnerable to fraud, as there is no clear accountability or strategic approach to mitigating fraud risks. Without fraud prevention being prioritized or mandated at the board level, it often becomes a secondary consideration, overshadowed by operational demands. As a result, fraud prevention may be reactive rather than proactive, leading to delayed responses, higher costs associated with fraud incidents, and missed opportunities to implement preventative measures.
- In 4% of organizations, **internal audit teams** take on the responsibility of fraud prevention within AP. Such teams are objective and skilled in risk assessment and controls testing. However, internal audit functions may not always have the capacity to address fraud risks on an ongoing basis, and their focus may be more on periodic assessments rather than daily vigilance.
- Just 2% rely on **external consultants or third-party vendors** for fraud prevention in AP. This is low, considering external providers can offer access to specialized expertise, advanced tools, and a broader perspective on industry best practices. Leveraging third-party support allows organizations to address specific fraud challenges and supplement their internal efforts, providing an opportunity to enhance fraud prevention strategies with targeted resources and solutions.

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.

Fraud Prevention Measures in AP Departments

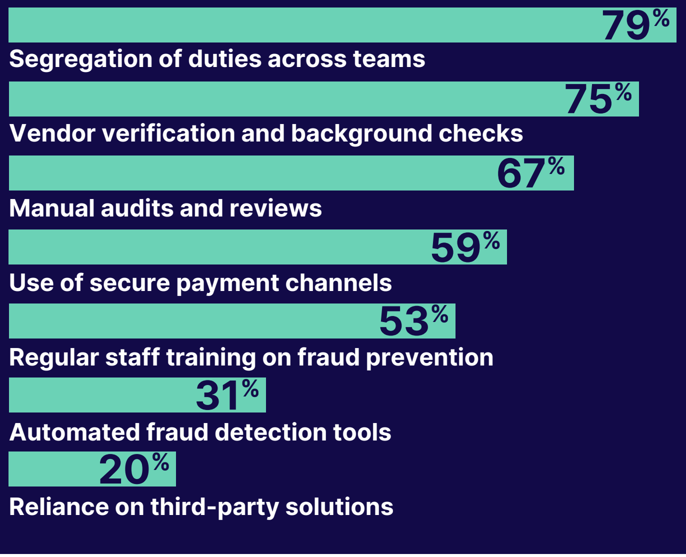
The following insights from our survey show the tools and practices organizations are currently using to mitigate fraud risk within their AP operations.

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.

Sponsored by basware Now it all just happens™

Written by sharedserviceslink

Which fraud prevention measures does your organization currently have in place?



1. Segregation of Duties Across Teams

The most widely adopted measure among AP departments is **segregation of duties**, with 79% of respondents using this control to reduce fraud risk. By ensuring that no single employee has control over multiple stages of a financial transaction (such as approval, processing, and reconciliation), organizations can reduce the opportunity for fraud.

2. Vendor Verification and Background Checks

A solid majority (75%) also implement **vendor verification and background checks**. This proactive measure helps AP teams ensure that they are transacting with legitimate, reliable vendors. Background checks and periodic verification help to identify red flags, such as inconsistencies in vendor information or irregularities in past transactions, providing a safeguard against fraud.

3. Manual Audits and Reviews

Manual audits and reviews remain a common practice, with 67% of AP departments relying on this approach. While periodic audits are a valuable tool for identifying issues, they leave gaps between reviews where fraudulent activity can go undetected. With the volume of transactions increasing and fraud tactics becoming more sophisticated, manual methods struggle to keep pace. This growing challenge highlights the need for automated solutions that can provide continuous monitoring, detect threats in real time, and address vulnerabilities before they escalate.

4. Use of Secure Payment Channels

Using **secure payment channels** is another measure adopted by 59% of respondents. Secure payment channels reduce the likelihood of payment fraud by providing additional layers of authentication and controls.

5. Regular Staff Training on Fraud Prevention

53% of respondents cited **regular staff training on fraud prevention** as part of their strategy. As fraud tactics evolve, continuous training ensures that employees remain vigilant and are aware of new fraud schemes, including those leveraging GenAI. AP teams must also keep up to speed with the commercial tools available to combat fraud.

6. Automated Fraud Detection Tools

Just fewer than a third (31%) of AP departments use automated fraud detection tools to identify and prevent fraud. However, in our previous research report, *From AI to ROI – CFOs and the Fast Track to Value*, we found that 92% of businesses that had implemented AI tools to support their AP process had seen faster identification of suspicious or fraudulent activity. Automated tools monitor transactions at scale, identify patterns of fraudulent behavior, and reduce the burden on AP staff by catching anomalies in real time, helping with preventative detection.

7. Reliance on Third-Party Solutions

Some organizations (20%) **turn to third-party solutions** to help manage fraud prevention efforts. External vendors often offer specialized tools and expertise in fraud detection and risk management, which can be especially valuable for companies with limited internal resources.

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.

Conclusion

This research illustrates how reliant large-scale organizations are on traditional internal controls, such as segregation of duties and vendor verification, as well as secure payment practices. The relatively low adoption of automated fraud detection tools suggests that most organizations are still in the early stages of modernizing their fraud prevention efforts.

As fraud tactics become more sophisticated, investing in advanced technologies and external expertise will become increasingly necessary to stay ahead of fraud threats.

Action Plan

Our 2024 survey reveals that 68% of organizations have faced fraud attempts, highlighting the urgent need for enhanced security measures across AP departments.

How can AP teams better safeguard their organizations?

1. **Embrace Automation and AI-Powered Detection:** Invest in intelligent automation to reduce the manual effort required for fraud detection and ensure AP teams are equipped to identify threats as they arise.
2. **Strengthen Cross-Functional Fraud Prevention Teams:** The most resilient AP departments are those that treat fraud prevention as a core operational function rather than an isolated task. This means developing dedicated fraud prevention teams, investing in regular staff training, and fostering cross-departmental collaboration. Collaborate with IT, legal, finance, and external experts where possible, leveraging diverse expertise to build a comprehensive fraud prevention framework. However, collaboration is only effective when you have accurate information that can be shared across departments. Fraud prevention relies on real-time data visibility across all ERPs.
3. **Promote a Culture of Vigilance and Education:** Regular training on emerging fraud tactics will keep AP teams informed and prepared to detect sophisticated threats.
4. **Seek External Support When Needed:** For organizations without dedicated AP fraud prevention teams, engaging external experts can be an effective way to bridge the gap. Third-party providers offer specialized tools, expertise, and scalable solutions to help identify and mitigate fraud risks. Many risks occur from having multiple source systems for vendor data, multiple AP processes and systems. Having a single tool used in AP and finance can give your organization a single source of truth. Leveraging these resources ensures your organization has the necessary support to stay ahead of evolving threats, even with limited internal capacity.

Looking ahead, organizations that embrace these solutions while maintaining flexibility in their approach will be best positioned to protect their financial integrity. The key lies not just in implementing individual measures, but in creating a cohesive strategy that strengthens both security and operational excellence.

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.

About **Basware**

Basware is how finance leaders in global enterprises can finally automate their complex, labor-intensive invoice processes and stay compliant with regulatory change. Our AP automation and invoicing platform helps you achieve a new level of efficiency – in a matter of months – while reducing errors and risks. We bring a unique combination of true automation, complete coverage, and deeper expertise to make it all just happen for our customers. That's why the world's most efficient AP departments rely on Basware to handle millions of invoices per year. **Basware. Now it all just happens.**

About **sharedserviceslink**

The sharedserviceslink is the world's largest community for finance shared services professionals. Forty thousand Friends have full access to our current and archived webinars, e-books, guides, white papers, reports and roundtables. Each year, twenty technology providers keen to win the finance shared services market, partner with sharedserviceslink to foster connections to expand their adoption.

For more content like this, please visit **www.sharedserviceslink.com** and remember to sign up as a Friend.

Listen to the full webinar here.

About **AP Protect**

AP Protect is the ultimate solution for finance leaders combating duplicate payments, potential errors, and fraud risks. Now, you can maximize your working capital without changing your existing processes.

Key benefits of Basware AP Protect:

- Prevent Overpayment: Proactively identify errors and prevent overpayment funds.
- Fraud Prevention: Highlight fraudulent vendors and questionable transactions with invoice analysis.
- Vendor Analysis: Use insights to remove the root causes of overpayment and fraud in the vendor master data.

Learn more about **AP Protect**

DISCLAIMER: All writers' opinions are their own and do not constitute financial or investment advice in any way whatsoever. Nothing published by sharedserviceslink constitutes an investment recommendation, nor should any data or content published by sharedserviceslink be relied upon for any investment activities. sharedserviceslink strongly recommends that you perform your own independent research and/or speak with a qualified consultant before making any investment decisions.