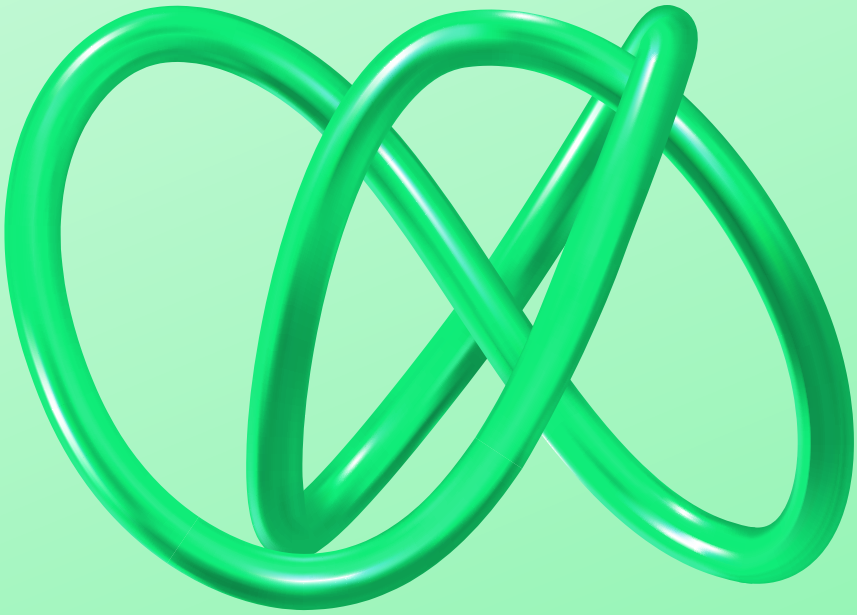
billtrust

WHITE PAPER

Raising the red flag

What finance leaders need to know about accounts receivable fraud schemes and how to fight them



Contents

Introduction

5-50%

Estimated rise in fraud since January 2022, according to fraud teams

Source: Sift

94%

of companies are investing in digital technologies in at least one area of payments and finance

Source: PYMNTS/Corcentric

Business billing and payments have undergone a massive shift over the past few years. From the expedited movement to digital channels to a volatile economic environment, finance leaders are grappling with how to address change to meet customer needs and address internal processes with care.

> One concern comes up in nearly every scenario: fraud.

That's because business fraud, a perpetual issue, is on the rise. In fact, 68% of trust and safety (cybersecurity) experts[1] have reported at least a 5% increase in fraud since January 2022, with some spikes as high as 50%.

In addition, the rapid acceleration of digital accounts receivable (AR) and accounts payable (AP) processes has led to added scrutiny. Ninety-four percent[2] of companies indicate they are investing in digital technologies in at least one area of payments and finance, with another 87% planning to invest in the future.

While these digital-first approaches bring efficiencies, they also require new fraud mitigation strategies. The more that finance functions go digital, the more protections are needed to support safe business operations.

> The more that finance functions go digital, the more protections are needed to support safe business operations.

What fraud costs, and how it happens

Fraud has always been a consideration for businesses, so why is the emphasis increasing now? For one, the rate of fraud continues to climb. A recent study from the Association of Certified Fraud Examiners indicated that organizations lose 5% of revenues to fraud each year, with the average loss per case nearing $1.8 million. [3]

The same study found that 27% of all occupational or internal frauds stem from accounting (12%) and operations (15%) departments, indicating additional checks and balances are necessary to mitigate this type of fraud.

The good news? Businesses are responding: 85% of chief financial officers (CFOs) report current or future plans to invest in fraud prevention and digital risk management technologies.[4]

But to address the full spectrum of potential business fraud, business leaders must address a wide number of scenarios, including:

- Internal fraud
- External attacks
- Collaboration between internal and external parties

In its Global Economic Crime and Fraud Study 2022, PwC concludes that 43% of fraud stems from an external perpetrator, 31% is from an internal party or parties, and another 26% is a result of collusion between the two. Addressing these shifts means breaking down internal departments and identifying specific risk factors for each.

58%

of payment professionals reporting that their AP department was targeted by email scams.

Source: Association for Financial Professionals

2 in 5

business say their IT and AP teams collaborate to fight fraud.

Source: Medius

Accounts payable fraud schemes

Outside fraud attacks frequently target accounts payable (AP) departments and their employees precisely because they have access to funds release.

For example, the Association for Financial Professionals (AFP) called out that these departments are most susceptible to BEC fraud, with 58% of payment professionals reporting that their AP department was targeted by email scams.[5]

Targeted invoice fraud also creates a major issue for businesses. A recent report revealed an average estimated annual cost of $280,000 per company over the past 12 months.[6] In addition, 95% of businesses have been aware of invoice fraud, and the average finance team has spotted 12 cases in the past year.

Why? Part of the issue lies in the fact that IT and AP teams work in silos in most organizations. The same study reported that the responsibility to detect and prevent false invoice activity is not shared, with only two in five businesses reporting collaboration.[7]

As primary targets of fraudulent activity, AP teams must be vigilant in monitoring for new attacks and training their teams to identify potential scams as they arise. But while it's an important approach, adding another task to a team's ever-increasing workload becomes a challenge for finance leaders. Automation is one tool that can help relieve the burden.

> AP teams need to be vigilant in monitoring for new attacks and training their teams to identify potential scams.

Accounts receivable fraud schemes

Fraud may not be as prevalent on the accounts receivable (AR) side, but it is on the rise. AFP reports a slight increase in AR fraud from 2020 to 2021 (3% to 5%) and lists it among the top six departments most vulnerable to BEC.[8]

From tactics like false checks, check kiting and check lapping to skimming sales and more, AR fraud abounds. That's why, as previously noted, 85% of CFOs are prioritizing fraud controls for incoming payments.[9]

In many cases, this type of fraud is perpetrated internally, with employees working the systems they know.

- **Asset misappropriation,** which involves an employee stealing or misusing the employer's resources, is the most common, accounting for 86% of cases.[10]
- **Financial statement fraud,** when a fraudster intentionally causes a material misstatement or omission in the organization's financial statements, only represents 9% of the total cases but are the costliest to the organization, with a median loss of $593,000.[11]
- **Kiting,** when an employee steals funds and transfers the money from one bank account to another before year-end.

Further, identifying this type of fraud may be difficult. In most cases, a lack of internal controls opens the door to AR fraud, with 29% of victim organizations reporting they did not have adequate mechanisms in place to guard against it. When controls were put in place, fraudsters were able to override those safeguards in 20% of cases.[12]

Businesses need to create checks and balances to evaluate and validate internal approvals and signoffs. Creating a workflow that engages technology and enables input from more than one staff member will help catch abnormal transactions and flag any issues.

> In many cases, [accounts receivable] fraud is perpetrated internally, with employees working the systems they know.
>
> Types of AR fraud committed by employees:
>
> 1. Bogus statements
> 2. Check skimming
> 3. Customer data phishing
> 4. Fictitious accounts and sales
> 5. Forced balancing
> 6. Fraudulent write-offs
> 7. Lapping and kiting
> 8. Payment diversion
> 9. Refund skimming

3 to 5%

Increase in AR fraud between 2020 and 2021

Source: Association for Financial Professionals

86%

of AR fraud cases are classed as asset misappropriation

Source: Association of Certified Fraud Examiners

Four ways you can mitigate AP and AR fraud

With fraud levels high and increasing on both the AP and AR sides, financial leaders have a lot to consider as they respond to market demands and build out digital systems.

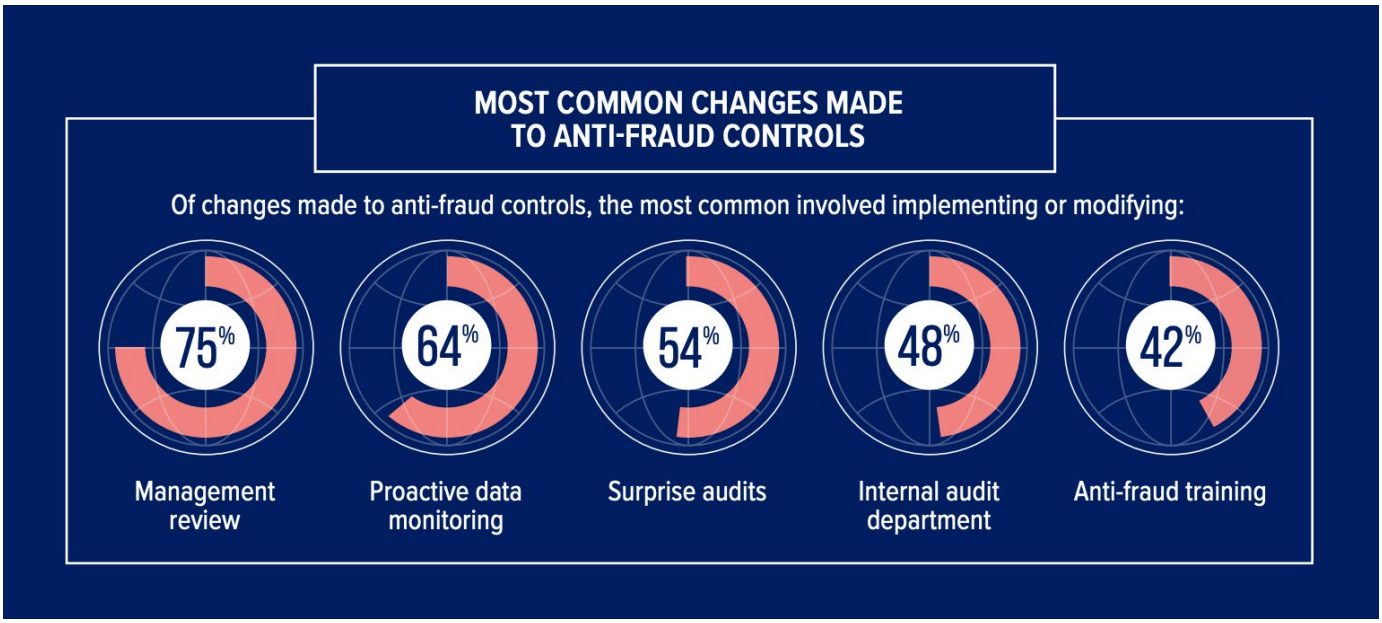
For example, with nearly half of occupational fraud potentially prevented with a stronger system of anti-fraud controls, small steps may have a big impact for the business.[13] As the PYMNTS report, "The Overlooked Importance Of Securing Incoming Payments," recently noted: "If done right, a streamlined and secure AR system would limit the ability of rogue employees as well as external fraudsters to steal funds."[14]

With that in mind, financial professionals should take the following steps for shoring up their AP/AR operations:

1. **Evaluate current processes and identify places where automation may create additional safeguards.** According to Billtrust research, AR teams interact with an average of 11 to 20 customer portals and must be proficient with 11 to 15 AP automation platform brands.[15] By making changes to how AP/AR operations are managed, you can lessen entry points for fraud activity and enhance efficiency in the process.
2. **Automate systems and layer them with fraud detection.** Once you've identified areas of opportunity, you should engage with a partner who can support the development of an efficient digital workstream for AP and AR tasks. Identify areas where internal controls may be needed and/or additional external support may be warranted to stave off fraud.
3. **Create internal checkpoints and dual sign offs for staff.** While it may create an added layer of approval, incorporating dual review of AP and AR activity may help identify any red flags for potential fraud. For example, with BEC, if two parties must review the request prior to any money being sent, it will create an added layer of scrutiny before payment. On the AR side, having a secondary review of materials in place—even a cursory one—may create a natural hesitancy for employees to act in a fraudulent way and enable you to more quickly recognize any outlier activity.
4. **Develop staff training.** The concept of "if you see something, say something" only applies if staff know what to look for in a particular scenario. Fraud training can give the necessary guidance to teams to help them in recognizing unusual activity.

Third-party providers offer tremendous opportunities to automate and digitize processes while supporting fraud mitigation. Having a trusted partner to help in navigating not only the automation but the security elements associated with it can go a long way in ensuring that as new workflows are created, fraud mitigation checkpoints are incorporated. Working with a provider and internal team members, financial professionals can set themselves up for future success in minimizing fraud impacts.

Association of Certified Fraud Examiners graphic[16]



Conclusion

> While fraud attacks continue to climb, you have a host of resources at your disposal.

By approaching AP/AR processes with a fresh set of eyes and identifying areas of weakness, financial professionals can anticipate issues and identify a path to greater operational safety.

In addition, new tools and resources continue to arise that will help ensure businesses remain one step ahead of fraud. Incorporating more robust AP/AR fraud detection processes will ready you and your team for whatever new market dynamics emerge. And in today's dynamic landscape, preparation supports success.

References

1. Sift. How to Build Resilient Fraud Management Strategies. https://pages.sift.com/rs/526-PCC-974/images/Ebook_Sift_How-to-Build-Resilient-Fraud-Management-Strategies.pdf
2. PYMNTS and Corcentric. Digitization Strategies: How CFOs Are Prioritizing Digital Payments To Maximize Efficiency. https://www.pymnts.com/wp-content/uploads/2022/11/PYMNTS-Digitization-Strategies-November-2022.pdf
3. Association of Certified Fraud Examiners. Occupational Fraud 2022: A Report to the nations. https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf
4. PYMNTS and Corcentric. Digitization Strategies: How CFOs Are Prioritizing Digital Payments To Maximize Efficiency. https://www.pymnts.com/wp-content/uploads/2022/11/PYMNTS-Digitization-Strategies-November-2022.pdf
5. Association for Financial Professionals. Highlights: AFP 2022 Payments and Fraud Control Report. https://www.afponline.org/docs/default-source/registered/highlights_afp-2022-payments-fraud-and-control-report.pdf?sfvrsn=70a166b_2
6. Medius. The Financial Professional Census. https://www.medius.com/resources/financial-professional-census-report-2022/?utm_medium=Public%20Relations&pi_campaign_id=41503&utm_source=Cision&utm_campaign=Financial-Census-2022
7. Ibid.
8. Association for Financial Professionals. Highlights: AFP 2022 Payments and Fraud Control Report. https://www.afponline.org/docs/default-source/registered/highlights_afp-2022-payments-fraud-and-control-report.pdf?sfvrsn=70a166b_2
9. PYMNTS. 85% of CFOs Are Prioritizing Fraud Controls for Incoming Payments. https://www.pymnts.com/news/security-and-risk/2023/85-pct-of-cfos-are-prioritizing-fraud-controls-for-incoming-payments/
10. Association of Certified Fraud Examiners. Occupational Fraud 2022: A Report to the nations. https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf
11. Ibid.
12. Ibid.
13. Ibid.
14. PYMNTS and nsknox. The Overlooked Importance Of Securing Incoming Payments. https://www.pymnts.com/wp-content/uploads/2023/01/PYMNTS-B2B-Payments-Fraud-January-2023.pdf
15. Billtrust and Paradxes, Inc. The State of Accounts Receivable: The Journey to Modernize. https://www.billtrust.com/resources/white-papers/the-state-of-accounts-receivable-and-b2b-payments-the-journey-to-modernize
16. Association of Certified Fraud Examiners. Occupational Fraud 2022: A Report to the nations. https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

billtrust

Learn more

For more information on ways to streamline processes with security in mind, visit billtrust.com or contact our sales team.

ABOUT BILLTRUST

Billtrust is a leading provider of cloud-based software and integrated payment processing solutions that simplify and automate B2B commerce. Accounts receivable is broken and relies on conventional processes that are outdated, inefficient, manual and largely paper based. Billtrust is at the forefront of the digital transformation of AR, providing mission-critical solutions that span credit decisioning and monitoring, online ordering, invoice delivery, payments and remittance capture, invoicing, cash application and collections.

CORPORATE HEADQUARTERS

1009 Lenox Drive, Suite 101
Lawrenceville, New Jersey 08648
United States

HAMILTON

11 South Gold Drive, Suite D
Hamilton, New Jersey 08619
United States

SACRAMENTO

2400 Port Street
West Sacramento, California 95691
United States

GHENT

64/501 Moutstraat
Ghent OVL 9000
Belgium

AMSTERDAM

H.J.E. Wenckebachweg 200-III
Amsterdam AS 1096
Netherlands

KRAKÓW

ul. prof Michała Życzkowskiego 19
3 piętro
Kraków 31-864
Poland

PM-BT-WP7-v1