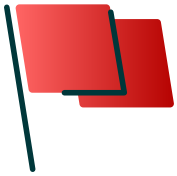
billtrust

WHITE PAPER

Trends in AP/AR fraud

How to spot them, and how to fight them



Fraud continues to grow as a primary business challenge.

80%

of businesses report being victims of a fraud attack.

Source: Association for Financial Professionals[2]

The 2024 Association for Financial Professionals' (AFP) Payments Fraud and Control Survey Report reveals that 80% of organizations said they were a victim of an attempted or actual fraud attack—an uptick of 15% over the previous year's findings. In addition, 30% of businesses were unable to recover funds lost due to fraud, significantly affecting their profitability.[1]

But what's triggering this increase? While the volume of attacks itself has climbed, perhaps more alarming is the level of sophistication being employed, leading to greater losses.

From more advanced takes on old types of fraud, like check washing, to the use of artificial intelligence (AI) technology for falsifying identities, fraudsters are introducing more convincing types of fraud. And that means your accounts payable (AP) and accounts receivable (AR) teams must remain on high alert.

"To thwart fraudulent activity in 2024, businesses need to deploy more sophisticated fraud protection solutions that harness the power of data and technology to mitigate risk and protect consumers."

Experian, 2024 Future of Fraud Forecast

What's new in fraud? An overview

By using more advanced technology, fraudsters can disguise their attacks in more authentic packaging. So, while not all the schemes are new, how they are perpetrated is shifting.

Unfortunately, your AP and AR teams must now work even harder to discern fact from fiction. Here are just a few trends in payments fraud and other types of scams:

Synthetic identity fraud became the fastest-growing type of digital fraud in 2023.

Advances in check fraud

Checks continue to be the number one source of payments fraud.[3] In fact, in February 2023, the Financial Crimes Enforcement Network (FinCEN) issued an alert on the nationwide surge in check fraud through the mail.[4] Long-existing schemes like check washing—removing and replacing the payee information and dollar amount on a legitimate check—now are aided by more advanced technology solutions that make the washed checks appear more authentic. Fraudsters are taking advantage of it, stealing business checks from the mail and altering them for financial gain.

Rise in business email compromise (BEC) via ACH

BEC, or when a fraudster tricks an employee into providing financial data or access via email, is a $55 billion industry, according to the FBI.[5] While BEC is an established form of business fraud, ACH credits have surpassed wires this year—for the first time—as the payment method that fraudsters most frequently target.[6]

According to AFP, "The shift to targeting ACH transactions through BEC is likely because ACH transactions are typically done in batches, and for the large payors, those transactions originate from Accounts Payable, which is considered to be most susceptible to BEC scams."[7]

Introduction of deepfakes

With advances in generative AI technology, fraudsters have moved beyond spoofed C-suite emails to impersonate those executives via voice and video. For instance, as reported in a recent Billtrust white paper, deepfakes impersonating CFOs and business leadership are now being perpetrated over Zoom, Microsoft Teams, and other videoconferencing platforms. So far, only 1% of businesses report being targets of deepfakes,[8] but that number is expected to climb rapidly: Experian predicts this will be a key fraud area for businesses soon.[9]

Resurgence of synthetic identity fraud

Data breaches have triggered the loss of copious amounts of Personally Identifiable Information (PII) that fraudsters can use to create false identities. This type of synthetic identity fraud is a "long-game play," with fraudsters taking PII, establishing credible identities, and then applying them to defraud companies under assumed but nonexistent identities. Reports indicate that those scams, which have been building since the 2020 pandemic, are now coming to a head: In 2023, synthetic identity fraud became the fastest-growing type of digital fraud.[10]

6 steps to fight AP and AR fraud

New trends in finance fraud requires a new level of vigilance from finance professionals. Here are some ideas for how your finance team can mitigate risk as fraud becomes more complex.

1

Use advanced cash management solutions to counter check fraud

With check fraud on the rise, businesses need to keep a close eye on any check payments they issue. Tools like Positive Pay, a cash management solution that financial institutions use to match checks submitted for clearing with checks the business has written, can make an impact.

Preliminary findings from a study from NEACH Payments Group recently revealed that 80% of corporates using Positive Pay witnessed a significant reduction in fraud.[11] Talk to your financial institution about the solutions available to you.

For the AR team, engaging with a technology partner that offers a comprehensive line of sight into days sales outstanding (DSO) may provide a much-needed deeper level of scrutiny in this fraud environment. Being proactive by keeping a closer eye on clients who most often pay by mailing a check may not only help you receive payment but also keep them from becoming a check fraud victim.

2

Create internal and external fraud controls

While the majority of fraud occurs externally—two-thirds of financial professionals report that payments fraud at their companies was the result of actions by an individual outside the organization—there is the potential for internal attacks.[12] Data shows that more than half of internal frauds occur due to lack of internal controls or an override of existing internal controls.[13]

AR teams are often tasked with monitoring for such activities as lapping, skimming, fraudulent write-offs, and more. Engaging with a technology partner whose solutions address best practices in internal procedures can help in supporting a locked-down internal operational environment.

3

Implement dual controls for all payments

Having more than one person review and sign off on outbound payments will introduce an added level of scrutiny on inbound requests. Consider it a double-check around the increasingly advanced, technology-forward fraud schemes out there.

4

Protect your data

In today's landscape, it's about making sure your data doesn't fall into the wrong hands, and that includes ensuring your technology partners stick to your organization's standards when it comes to AI.

When you engage with partners, require them to take these precautions:

- **Store data in cutting-edge cloud solutions** that are equipped with robust built-in security and governance features.
- **Adhere to stringent generative AI policies** that expressly prohibit the use of shared data for external training or any purposes outside the scope of their products and services.
- **Leverage trusted AI models** whose data usage policies are compliant with yours.

83%

of organizations expect to implement generative AI as part of their anti-fraud programs over the next two years.

Source: Association of Certified Fraud Examiners[15]

5

Educate your customers and partners

Requiring higher levels of authentication and implementing internal fraud systems can help protect your AP/AR processes, but taking that one step further and sharing your knowledge with your customers and partners can help them protect themselves.

For example, letting them know how you will and won't communicate with them about outstanding invoices will allow them to flag any potential fraud that could appear to be from your organization.

6

Partner with solution providers that offer advanced fraud detection capabilities

Today, 91% of organizations use data analysis techniques as part of their anti-fraud programs,[14] and generative AI continues to develop in sophistication. Seek out AP/AR partners who are committed to harnessing the power of AI to provide the data you need in the fight against cyber fraud.

As fraud gets more advanced, so do the systems designed to thwart it. More than ever, businesses need advanced technological solutions to help support their fraud and risk mitigation efforts. Identifying a partner that uses the latest fraud technology and makes your organization's safety a top priority will ensure a more secure, efficient and profitable financial process for your business now and into the future.

For more information on how Billtrust can best serve your needs, visit billtrust.com.

Bringing AR peace of mind to security firms

When leading security and data firms turn to one company for their AR needs, it speaks volumes about the built-in safety that the company's established payments process offers.

For instance, when high-tech security solutions firm Alertis was looking for a partner to structure and automate its debtor management, the company turned to Billtrust. And when a global business dedicated to storing, protecting, and managing information and assets needed an automated billing and payments solution to move customers toward electronic payments while also providing an avenue for mailed ones, it chose Billtrust.

That's because Billtrust takes security seriously. We provide a systematic approach to AI that sets the foundation for future innovation, keeping data security and privacy top of mind. Billtrust offers cross-product analytics, generative AI for intuitive queries, and personalized alerts, revolutionizing data-driven decision-making and customer communications.

"Our tools apply analytics and AI to customer datasets, helping users gain unparalleled insights and a 360-degree view of their entire order-to-cash process, including payment trends, buyer behavior, risk analysis, and anomaly detection," says Ahsan Shah, Billtrust Senior Vice President of Data Intelligence.

References

1. AFP. "2024 AFP Payments Fraud and Control Survey Report," April 2024, p. 6. https://www.afponline.org/docs/default-source/registered/2024-afp-payments-fraud-survey-key-highlights.pdf
2. AFP. "2024 AFP Payments Fraud and Control Survey Report," April 2024, p. 6. https://www.afponline.org/docs/default-source/registered/2024-afp-payments-fraud-survey-key-highlights.pdf
3. AFP. "2024 AFP Payments Fraud and Control Survey Report," April 2024, p. 6. https://www.afponline.org/docs/default-source/registered/2024-afp-payments-fraud-survey-key-highlights.pdf
4. FinCEN. "FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail," February 27, 2023, https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf
5. Federal Bureau of Investigation Public Service Announcement. "Business Email Compromise: The $55 Billion Scam," September 11, 2024, https://www.ic3.gov/Media/Y2024/PSA240911
6. AFP. "2024 AFP Payments Fraud and Control Survey Report," April 2024, p. 6. https://www.afponline.org/docs/default-source/registered/2024-afp-payments-fraud-survey-key-highlights.pdf
7. AFP. "2024 AFP Payments Fraud and Control Survey Report," April 2024, p. 12. https://www.afponline.org/docs/default-source/registered/2024-afp-payments-fraud-survey-key-highlights.pdf
8. AFP. "2024 AFP Payments Fraud and Control Survey Report," April 2024, p. 16. https://www.afponline.org/docs/default-source/registered/2024-afp-payments-fraud-survey-key-highlights.pdf
9. Experian. Press Release. "Experian releases 2024 Future of Fraud Forecast," February 13, 2024, https://www.experianplc.com/newsroom/press-releases/2024/experian-releases-2024-future-of-fraud-forecast-
10. Transunion. "Public Sector Omnichannel Fraud in 2023," June 24, 2024, https://www.transunion.com/blog/public-sector-omnichannel-fraud-2023?atvy=%7B%22248034%22%3A%22Experience+A%22%7D
11. NEACH Payments Group. LinkedIn post from CEO Sean Carter. Accessed September 23, 2024. https://www.linkedin.com/posts/sean-carter-aap-aprp-ba87104_with-annual-check-collection-by-the-federal-activity-7234632336871448576-eaMo?utm_source=share&utm_medium=member_desktop
12. AFP. "2024 AFP Payments Fraud and Control Survey Report," April 2024, p. 16. https://www.afponline.org/docs/default-source/registered/2024-afp-payments-fraud-survey-key-highlights.pdf
13. Association of Certified Fraud Examiners. "Occupational Fraud 2024: A Report to the Nations," 2024. https://legacy.acfe.com/report-to-the-nations/2024/
14. Associations of Certified Fraud Examiners. "Anti-Fraud Technology Benchmarking Report," 2024. https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report
15. Associations of Certified Fraud Examiners. "Anti-Fraud Technology Benchmarking Report," 2024. https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report

billtrust

Learn more

Visit billtrust.com or contact our sales team.

ABOUT BILLTRUST

Finance leaders turn to Billtrust to get paid faster while controlling costs, accelerating cash flow and maximizing customer satisfaction. As a B2B order-to-cash software and digital payments market leader, we help the world's leading brands move finance forward with AI-powered solutions to transition from expensive paper invoicing and check acceptance to efficient electronic billing and payments. With more than $1 trillion invoice dollars processed, Billtrust delivers business value through deep industry expertise and a culture relentlessly focused on delivering meaningful customer outcomes.

CORPORATE HEADQUARTERS

11D South Gold Drive
Hamilton Township, New Jersey 08691
United States

SACRAMENTO

2400 Port Street
West Sacramento, California 95691
United States

GHENT

Moutstraat 64 bus 501
9000 Ghent
Belgium

AMSTERDAM

Duivendrechtsekade 80B
1096 AH Amsterdam
Netherlands

KRAKÓW

ul. prof Michała Życzkowskiego 19
Kraków 31-864
Poland

PM-BT-WP24-v1