The State of Business Payment Security In The U.S.

2024 Report conducted by Trustmi

Table of Contents

Executive Summary

Business payment fraud has emerged as a paramount concern for businesses of all sizes. According to the 2023 Association for Financial Professionals (AFP) Payments Fraud and Control Survey Report, conducted by J.P. Morgan, 65% of surveyed companies, regardless of size, reported encounters with B2B payment fraud. The financial risk and potential damage to trust and reputation make this a significant business issue.

The root of B2B payment fraud lies in the vulnerabilities inherent in companies' payment processes. These vulnerabilities stem from:

Highly complex procedures / Finance teams struggle with multiple, siloed tools and lack end-to-end visibility over payment processes.

Susceptibility to human error / A high volume of invoices processed manually across hundreds or thousands of partners is extremely vulnerable to human errors.

Lack of visibility / Due to legacy systems and manual processes, financial professionals lack insight into the security posture of their payment processes.

Limited automation / Without robust automation, finance teams cannot detect payment fraud promptly, compounding the complexity and financial loss.

To get the latest pulse on the state of business payment processes and security measures, Trustmi recently conducted a survey of 516 finance professionals. The findings show that the lack of end-to-end automation leads to a steady stream of human errors in payment processes. The survey also shows a significant shift in cyberattacks. Traditional business email compromise (BEC) attacks still dominate; however, with the advent of generative AI, bad actors are unleashing more sophisticated attacks.

The threat of B2B payment fraud presents a danger to businesses across all sectors and sizes. The vulnerabilities exposed in current payment processes, from manual procedures to human error to lack of visibility, combined with an expanding attack surface, create a perfect storm for fraudsters to exploit.

As the financial and reputational stakes continue to rise, companies that fail to adapt and strengthen their defenses risk significant losses. By embracing innovative solutions and fostering a culture of security awareness, organizations can protect their assets, maintain trust with partners and customers, and stay ahead of the ever-evolving fraud landscape.

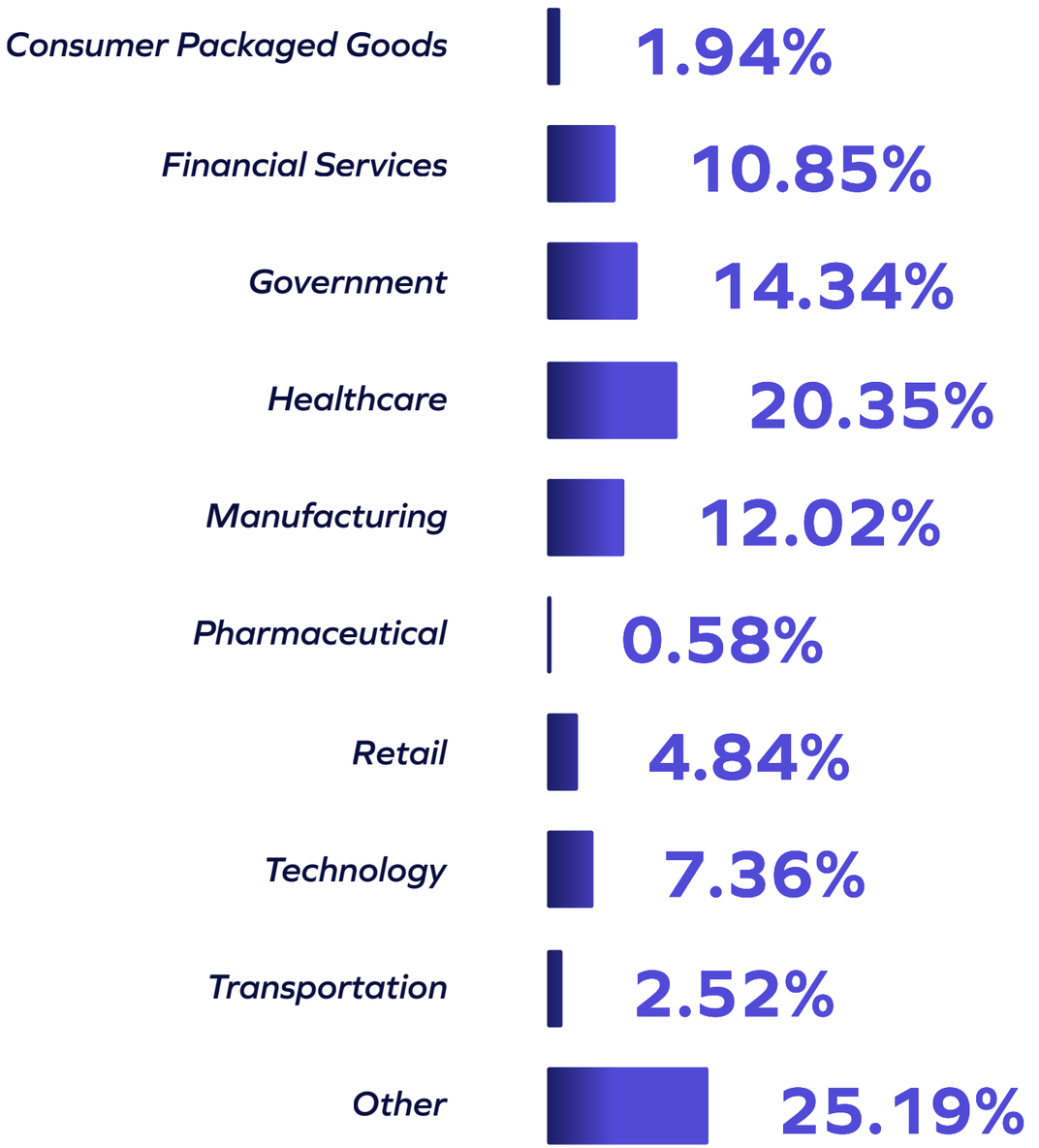
About the /

Participants

To accurately assess the state of business payment security, the survey targeted finance professionals in accounts payable, treasurer, finance manager, VP/director of finance, CFO, and other finance-related positions. A total of 516 respondents from diverse industries participated, including healthcare (20.35%), government (14.34%), manufacturing (12.02%), financial services (10.85%), and retail (4.84%).

Respondents /

516

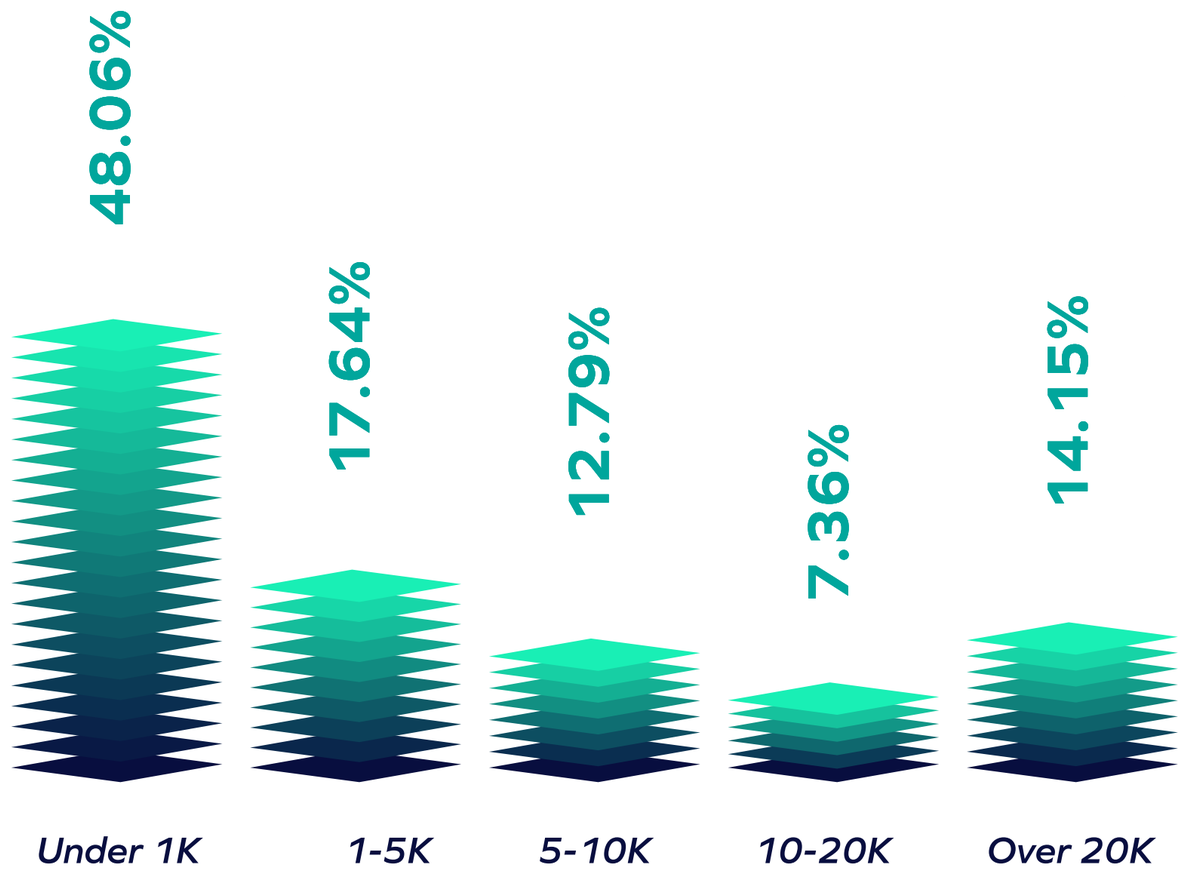


The Landscape

The complexity of a business's payment processes can increase an organization's susceptibility to attacks by providing more opportunities for attackers to exploit vulnerabilities. Industries such as manufacturing and retail with intricate procure-to-pay processes, numerous vendors, and a high volume of invoices are particularly vulnerable due to the complexity and potential for human error. According to the study, over 14% of organizations process over 20,000 invoices per month, and over 7% handle between 10,000 - 20,000 monthly. **This indicates that over one-fifth of companies are highly susceptible to attacks on their business payments due solely to the high volume of invoices they process each month.**

Organizations that frequently handle large financial transactions are also at greater risk due to the potential for significant financial gain. Additional factors that can increase the risk of attack include the use of online payment systems, the storage of large amounts of customer data (including payment information), and complex supply chains.

How many invoices do you process per month?

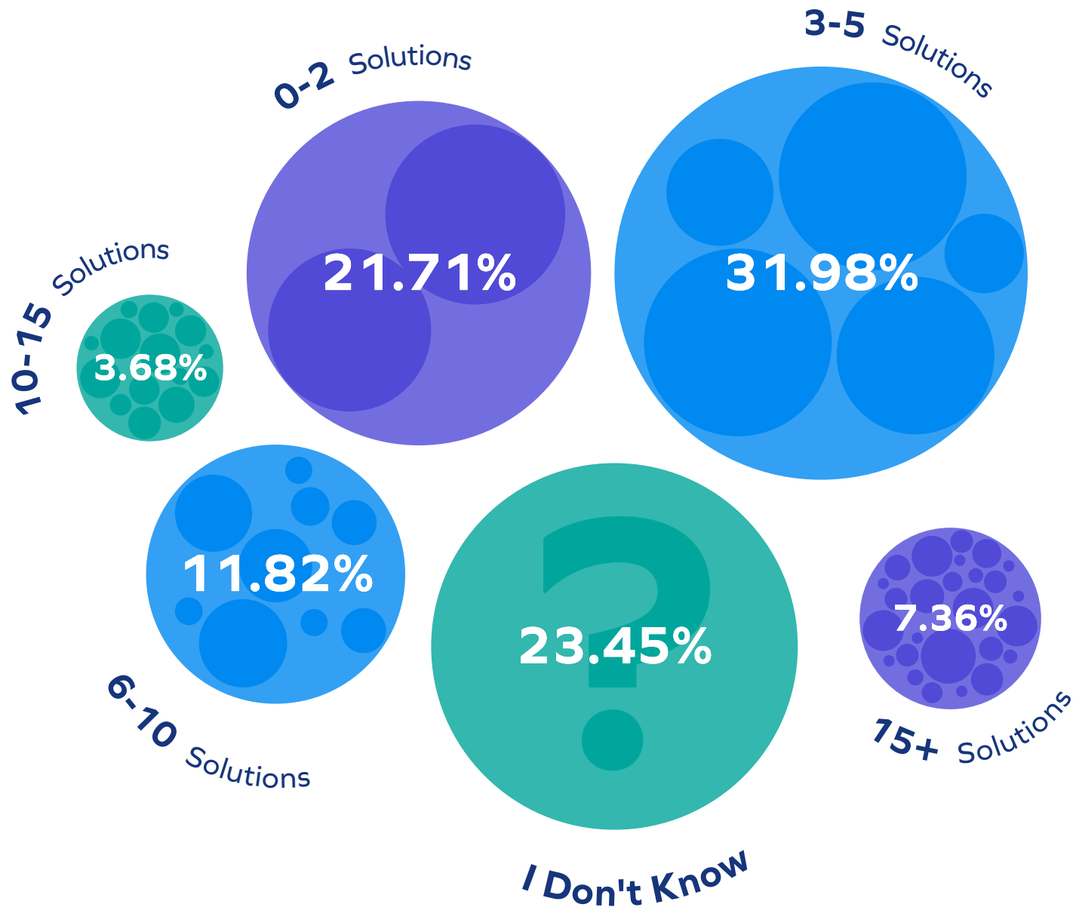


To combat increasingly sophisticated attacks on business payments, over 53% of organizations rely on five or fewer technology solutions including ERP and vendor management systems, AP automation technologies, and AP fraud detection tools.

More than 15% use 6 - 15 tools, while over 7% utilize more than 15 tools in their technology stack. Notably, more than 23% of respondents were unaware of the number of technology solutions involved in their payment processes.

Most organizations (nearly 58%) incorporate fraud prevention in their technology stack. Surprisingly, **almost 14% of organizations currently do not utilize this technology, leaving their payment processes vulnerable to attacks.** The absence of payment fraud technology exposes organizations to heightened risks of financial losses, compliance issues, and reputational damage, eroding trust among customers and partners.

How many technology solutions are involved in your payment processes?



Prevalent Challenges Plaguing Business Payment Processes

One key benefit of fraud prevention technology is automation, critical to protecting business payment processes. Automation is crucial in reducing human errors, enhancing security, ensuring regulatory compliance, and providing better visibility and control, making it an essential tool for safeguarding business payment processes.

For example, automated fraud prevention can:

Incorporate enhanced security measures / such as encryption, multi-factor authentication, and regular monitoring of access logs to protect against fraud and data breaches.

Facilitate compliance with regulations / like PCI DSS, GDPR, and AML, helping businesses avoid legal and financial risks.

Break down silos between roles and departments / enhancing visibility and control over payment processes, which is imperative to detecting and preventing unauthorized activities.

Reduce human errors in manual processes / such as duplicate payments or overpayments—that can result in significant financial loss.

Ensure there are no oversights or lapses / which often occur with manual processes.

Only 5% of organizations have completely automated their payment processes

Nearly 69% of organizations automate some or most of their payment processes

26% of companies still operate manual or somewhat manual payment processes

With progress being made to incorporate automation into payment processes, it is promising that nearly 50% of organizations have avoided payment fraud to date. Payment fraud can occur in various ways, such as phishing attacks, invoice fraud, and account takeovers. However, the same number either has experienced payment fraud (28%) or isn't sure (22%).

The lack of visibility highlights an ongoing issue among organizations, particularly finance teams. Several factors contribute to this visibility challenge, including:

The ongoing reliance on legacy systems and manual processes that cannot produce real-time data or comprehensive reporting, making timely fraud detection difficult.

Siloed financial systems, as information may be fragmented or inaccessible to those who need it.

Complicated workflows that hinder the ability to monitor payment processes effectively.

Lack of investment in advanced fraud detection and prevention technologies incorporating artificial intelligence and machine learning contributes.

Business Payment Security Realities

Types of Payment Fraud

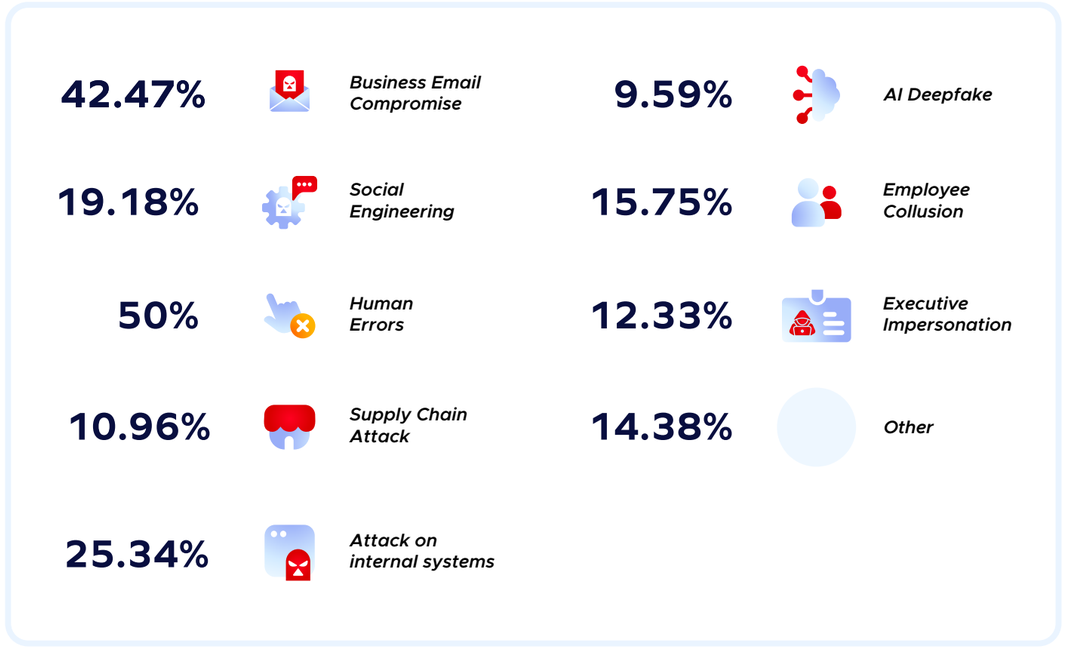
As organizations struggle to gain visibility across their payment processes and gradually adopt automation across their payment workflows, it is crucial to understand the main types of payment fraud and the consequences of inadequate security measures.

There are many sources behind business payment fraud. Two quickly gaining momentum include AI-driven deepfakes and executive impersonations. While relatively new tactics, **22% of organizations have already experienced payment fraud resulting from AI-driven deepfake (9.6%) and executive impersonation (12.3%) attacks.** Perhaps the most high-profile deepfake attack occurred in February 2024, when a multinational Hong Kong-based company lost $25 million to a complex phishing scam. Using publicly available videos on YouTube, scammers created elaborate deepfakes of the company's CFO and coworkers of the target.

Human error was the most common source of payment fraud revealed in this survey. In fact, **50% of organizations have experienced fraud due to human error,** which often stems from a company's reliance on legacy technologies that struggle to keep up with the increasing number of payment cycles and transaction volumes. This leads to human errors such as duplicate payments, lost invoices, and payments for incorrect amounts, highlighting the urgent need for more robust systems and processes.

BEC, or Business Email Compromise, is also a top cause of payment fraud. In a typical BEC scenario, perpetrators gain access to executive or decision-maker's emails to steal sensitive information and send fraudulent payment requests, among other actions. According to the research, **just over 42% have experienced a BEC attack.**

What caused your business payment fraud?



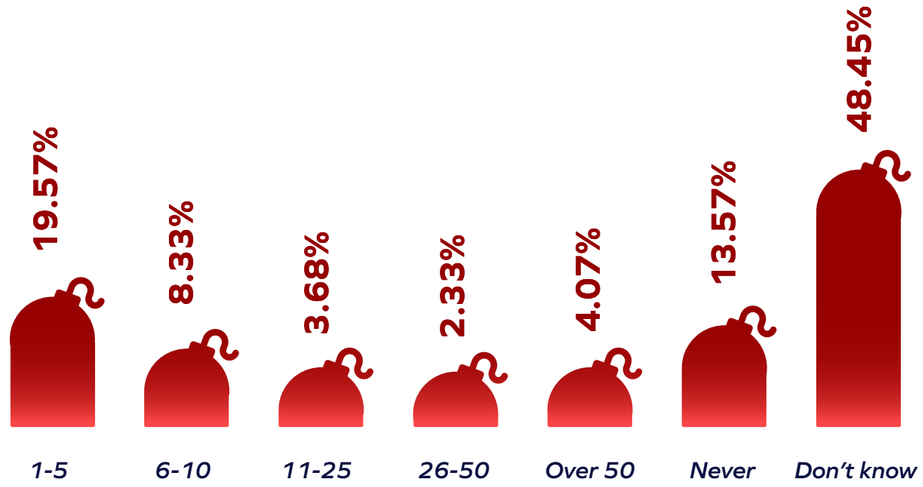
Perhaps the most concerning finding is the number of respondents who are unaware of the frequency of payment fraud attempts targeting their organizations in the past 12 months. **Forty-two percent admitted not knowing if their businesses had been targeted by a payment fraud attempt.** This group included CFOs, treasurers, and accounts payable professionals.

This lack of insight calls for a shift from siloed operations and outdated legacy solutions. Given the volume of business payments and the diversity and complexity of partner ecosystems, leading-edge finance teams are leveraging AI-powered business payment technology that delivers real-time visibility from vendor onboarding to payment release. With end-to-end visibility and automation, teams can quickly detect abnormal payment activities, prevent fraud from all attack vectors, and prevent loss from needless human errors.

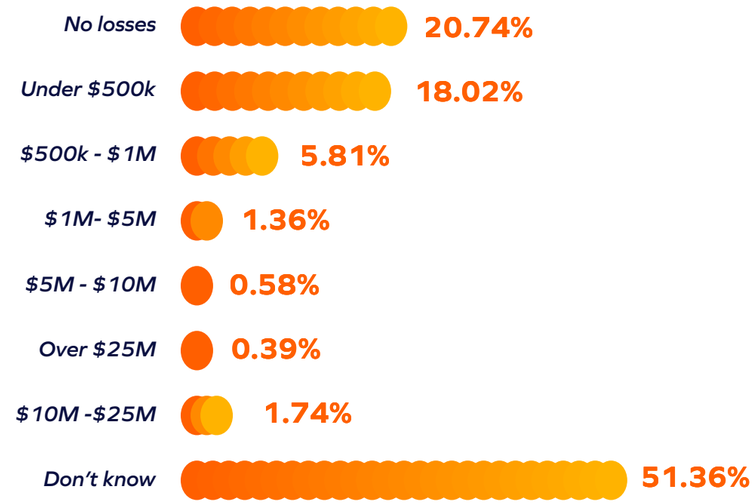
For those who successfully identified payment fraud incidents in the last 12 months, over 6% were targeted 25 times or more, and nearly 28% were attacked 1 - 10 times.

Lack of visibility continues to be an issue when determining financial loss from payment fraud. According to the survey, more than 51% of respondents don't know how much money their business has lost due to payment fraud over the last 12 months. This is especially troubling since financial planning and management are core elements of each finance professional's day-to-day job.

How many times has your organization been targeted with payment fraud attempts in the past 12 months?



How much money has your organization lost due to payment fraud in the past 12 months?



Conclusion

Organizations must recognize the financial impact and erosion of brand trust caused by payment fraud. Some lose millions of dollars annually. Despite this, many remain unaware of the losses incurred, highlighting the need for greater visibility and automated fraud detection technology.

The lack of insight necessitates a shift from siloed operations and legacy solutions to AI-powered payment technologies. Advanced business payment security systems provide end-to-end visibility, enabling finance teams to detect and prevent fraud more effectively, reduce human error, and stop financial loss. By implementing cutting-edge technology and fostering a culture of vigilance, organizations can protect their financial assets and ensure the integrity of their payment processes.

About Trustmi

Trustmi is the only end-to-end payment security solution that helps businesses protect their bottom line by eliminating losses from cyberattacks, internal collusion, and human error.

Trustmi's flexible and modular solution offers businesses complete control to use only the tools they need for securing their payment processes and managing their vendors. Founded in 2021 by Shai Gabay and Eli Ben Nun, Trustmi is headquartered in Tel Aviv with an office in New York City.

For more information visit /

www.trustmi.ai