trustpair

Fraud in the Cyber Era: 2024 Fraud Trends and Insights

Table of contents

With the collaboration of:

Baptiste Collot, CEO of Trustpair
Lee-Ann Perkins, Assistant Treasurer, Nacha Advisory Board member

Methodology:

- Respondents: 266
- Geography: USA
- Audience: Director and C-Level Finance and Treasury professionals
- Company size: Over $1B in revenue
- Field dates: from 11/07/23 to 11/13/23
- Research Organization: Cint

Executive Summary

With an alarming 83% of companies targeted by cyber fraud (activities such as hacking, deepfakes, highly sophisticated phishing schemes, etc.) in the last 12 months, corporate fraud has undeniably entered the Cyber Era. ChatGPT-generated text messages, hacked websites, and deep-fake phone calls are now the norm as fraudsters use cutting-edge technology and AI to move **faster and better than ever before**.

On top of the extreme financial losses - 36% of companies lost more than $1 million on average - fraud also damages relationships with customers, investors, and suppliers. Despite a clear acknowledgment of the rising tide of cyber fraud, with 67% of companies anticipating an increase in fraudulent activities in 2024, there is a concerning **lag in adopting adequate cyber fraud defenses.**

Only a fraction of companies have implemented comprehensive fraud prevention software, relying instead on traditional, less effective methods like double-checks and manual validations. This lagging response to growing cyber fraud highlights a critical need for **more proactive, automated measures to fight the challenges of cyber fraud**. This report sheds light on the key fraud trends and offers expert insights and takeaways companies can use to fight back against fraudsters in 2024.

> Fraud is now so elevated in complexity that we - as companies - need to elevate the solutions and controls to fight back.

Lee-Ann Perkins
Assistant Treasurer
Nacha Advisory Board member

#1 Payment fraud is surging

1

96%

of companies were targeted by **at least 1 fraud attempt**

2

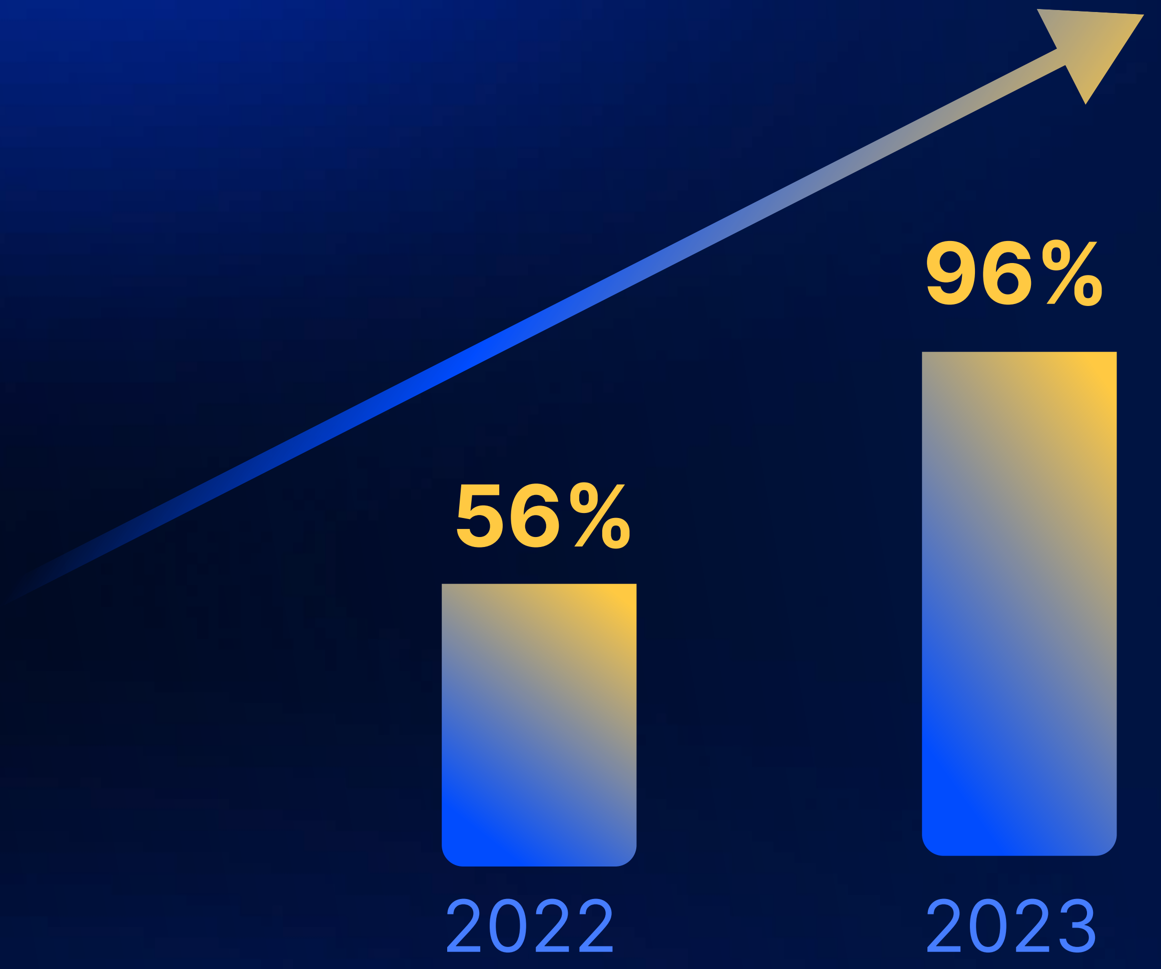
36%

of victims of successful fraud **lost more than 1M dollars**

3

+71%

is the increase of companies targeted by fraud in 2023 vs 2022



1 & 3 - How many payment fraud attempts has your organization been targeted by in the past 12 months? Respondents: 266
2- What was the average financial loss of successful fraud incidents you experienced? Respondents: 255

ANALYSIS

In 2023, fraud hit US companies harder than ever before. There was a 71% increase in the number of companies targeted at least once compared to last year. Most organizations (96%) were targeted at least once in 2023. **94% were targeted multiple times**, and 21% more than 10 times. A rise in cyber fraud is contributing to the rise in fraud attempts: In 2022, only 6 out of 10 companies were targeted by fraud.

Not only are fraudsters more aggressively targeting large companies, but they're also extremely successful. **Ninety percent of companies** that were targeted by fraud experienced at least one successful attack. In 78% of companies, fraud was successful multiple times.

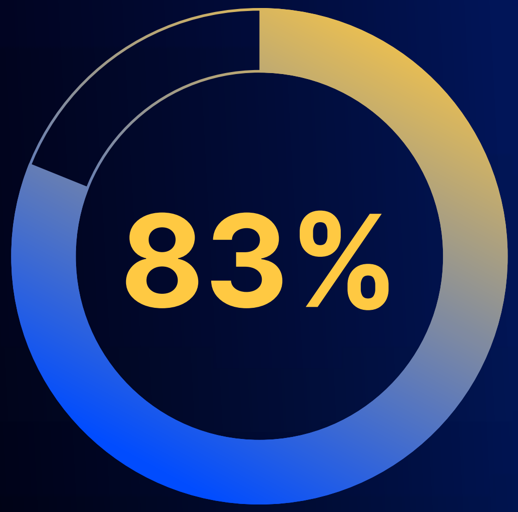
In addition, the average amount of financial loss is substantial. If the average loss amounts to $100,000 per fraud event, 36% of companies lost more than $1 million on average and 25% more than $5 million. These staggering numbers can be explained by the ever-changing nature of fraud: as cybersecurity and fraud become inextricably linked **fraud becomes more difficult to detect**. Fraudsters are increasingly savvy and fly under the radar. When fraud is finally spotted, it's generally too late. The damage is done and companies can't always recoup their losses.

> Cyber fraud is more complex to identify and goes undetected longer. This amounts to larger sums lost through fraud: fraudsters act in the dark and act multiple times before they're spotted.

Baptiste Collot
Co-Founder and CEO
Trustpair

#2 Fraud has entered the Cyber Era

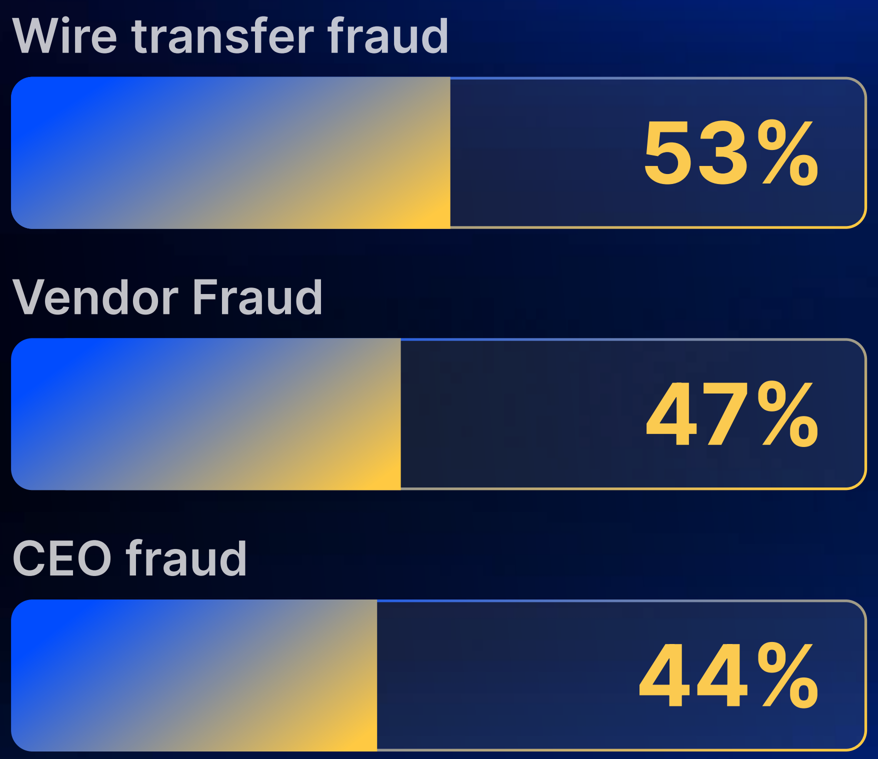
[1]



of companies were targeted by **cyber fraud**

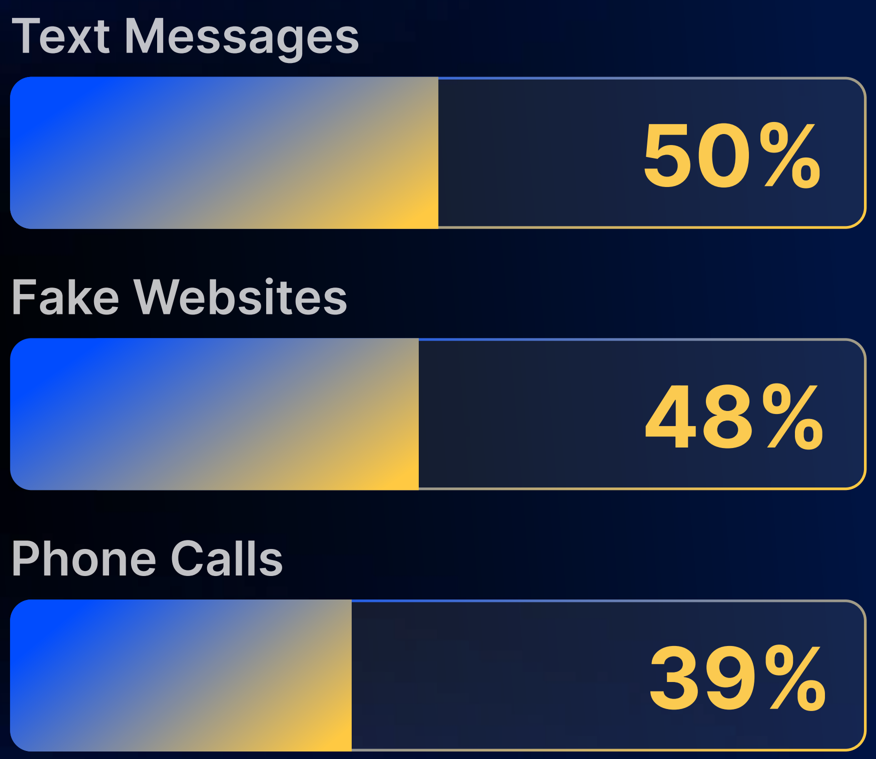
[2]

Top 3 **fraud types**



[3]

Top 3 **channels** used



1- Were any of the payment fraud attempts or successful attacks your organization experienced driven by cyber fraud? Respondents: 255
2- What types of fraud were you targeted by? Select all that apply. Respondents: 255
3- Which channels were used to perpetrate the attempts or successful fraud attacks in the past 12 months? Select all that apply. Respondents: 255

ANALYSIS

The nature of fraud has been changing over the last decade. From manual fraud handled by isolated fraudsters, we've moved to **industrial fraud with highly specialized and skilled fraudsters**. They use tools and techniques that are undetectable without the right safeguards. 83% of companies were targeted by cyber fraud in 2023. The most common channels used were text messages (50% of companies), fake websites (48%) and phone calls (39%). These channels are prioritized by scammers. Thanks to generative AI tools like ChatGPT, they can create close-to-perfect texts, emails, phishing websites, and deep-fake voices at a higher pace and scale than ever before.

Fraudsters also use new techniques for widely known fraud types like wire transfer fraud (53% of companies), vendor fraud (47%), and CEO or CFO impersonations (44%). The success of wire transfer fraud isn't surprising: wire transfer was indicated by 59% of companies as one of the payment methods most targeted by fraudsters.

Paper checks were less targeted than last year (26%) which isn't surprising considering its declining use in B2B payment. However, it's important to be aware of the risks that come with the shift from paper checks to electronic payments. Indeed, it means entering new vendor data in your database. This sudden and massive amount of data represents a risk for the company and an opportunity for fraudsters if companies don't regularly monitor their vendor data. It's one of the explanations for the drastic rise in cyber fraud.

> All these available AI solutions like ChatGPT that we use in our everyday lives make work easier, create efficiencies, and eliminate repetitive tasks and errors. But just as much as we're using these solutions for good, fraudsters are using them for their good too: to defraud our companies and get into our systems.

Lee-Ann Perkins
Assistant Treasurer
Nacha Advisory Board member

#3 The fraud domino effect

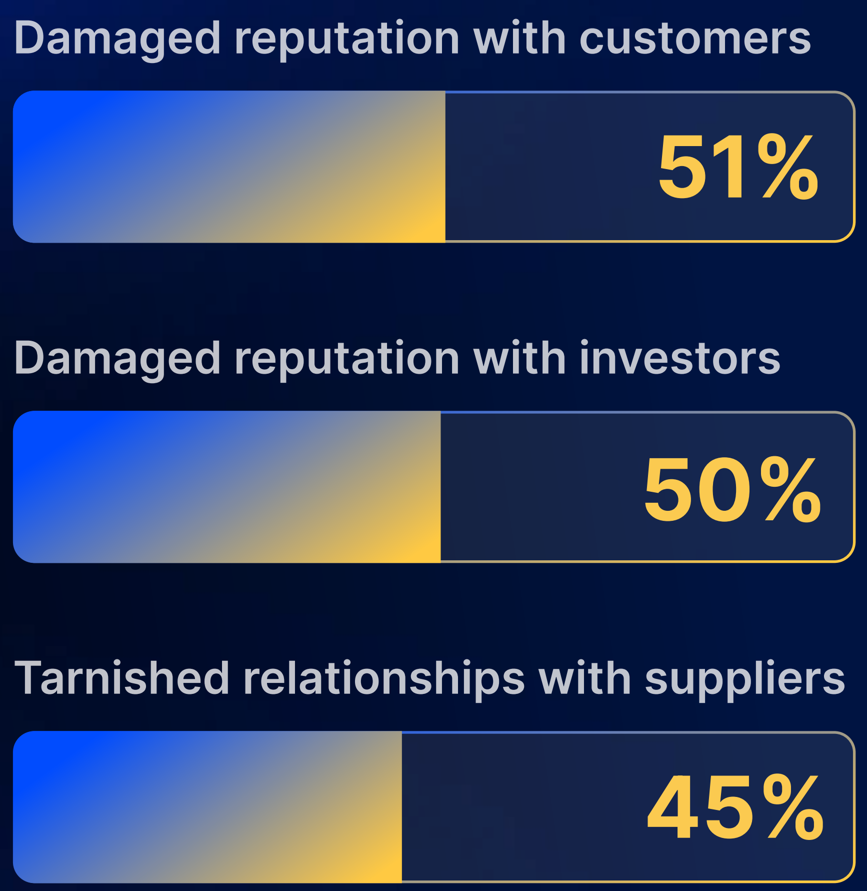
[1]

66%

of companies **would stop doing business with an organization** if it fell victim to payment fraud and lost its payment

[2]

Companies say one of the **top impacts of fraud** they're afraid of is:



1- Would you stop doing business with an organization if they fell victim to payment fraud and lost your payment? Respondents: 266
2- Outside of financial losses, what impacts of fraud keep you up at night? Pick your top three. Respondents: 266

ANALYSIS

Although the financial loss from payment fraud is significant, it's not the only impact companies worry about. For 51% of respondents, reputational impacts with customers or investors (50%) cause finance and treasury leaders to lose sleep. This can harm businesses further with **significant loss of business activity** in the long run.

45% of companies see tarnished relationships with suppliers as a possible consequence of fraud. This isn't surprising seeing how vendor fraud (47%) is one of the top three types of fraud. In cases of vendor fraud, fraudsters divert vendor payments to their accounts: vendors don't get paid on time - or at all - which can create **friction in the buyer-supplier relationship**.

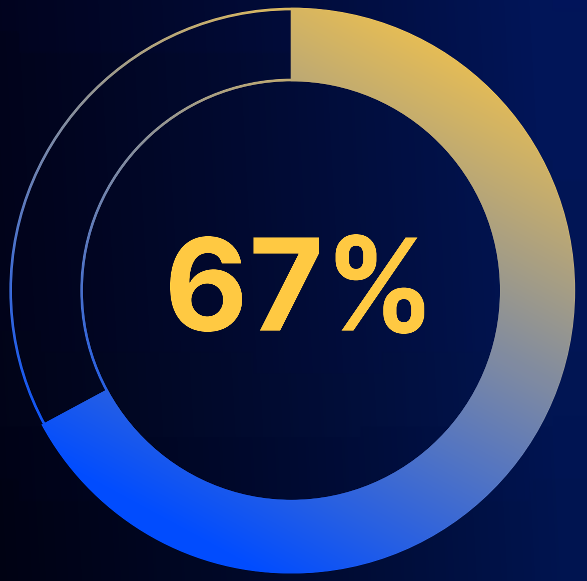
Perhaps the most striking number: 66% of companies would stop doing business with an organization if it fell victim to payment fraud and lost its payment. This alone shows the possible domino effect that fraud can have, far from the direct financial loss alone.

> One of our client's vendors got his email hacked. The fraudsters sent a change request by email. He paid two invoices to the fraudsters. The fraud took a long time to detect: the vendor thought payments were late.
>
> There was a trial. Our client blamed his vendor, saying the fake information came from its email servers. So these two companies that had worked together for many years ended up in court. This is one of the impacts of fraud that goes further than the financial loss

Baptiste Collot
Co-Founder and CEO
Trustpair

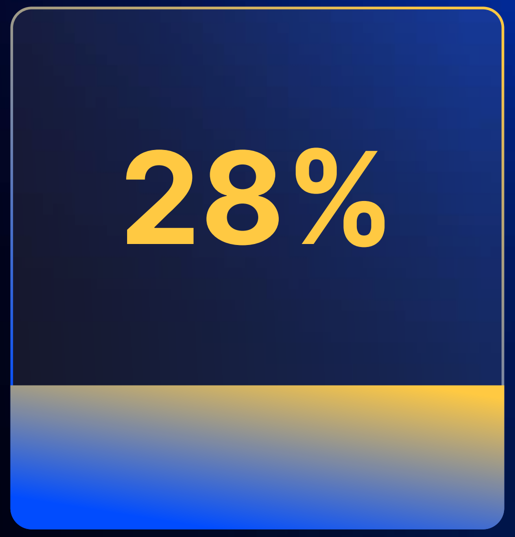
#4 Companies are trapped in a **“it won’t happen to me”** mindset

[1]



of companies expect fraud to **increase**

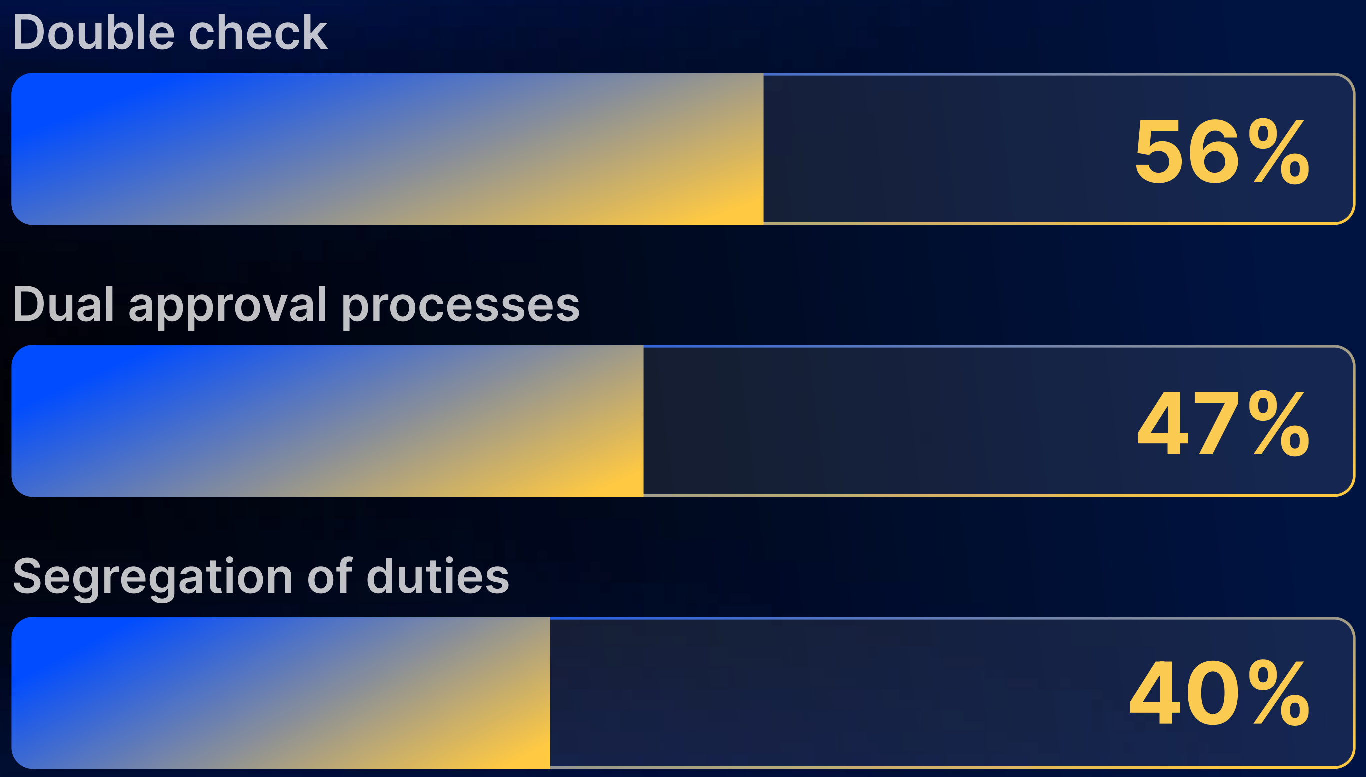
[2]



However, only 28% have fraud **prevention software**

[3]

The top **defenses** in place today are:



1- Do you expect payment fraud to rise in the next 12 months? Respondents: 266
2- What defense measures do you have in place to fight payment fraud? Select all that apply. Respondents: 266
3- What defense measures do you have in place to fight payment fraud? Select all that apply. Respondents: 266

ANALYSIS

The good news: companies are aware of the fraud risks. The bad news: companies don't realize how likely it is for fraud to happen to them. There's more companies can be doing to invest in the right tools and safeguards to fight fraud.

Sixty-seven percent of companies expect fraud to continue increasing in 2024. **Fraud and cybersecurity are increasingly intertwined**, which calls for modern tools and automation. However, only 28% of companies have fraud prevention software as a defense mechanism to help them keep up with rising cyber fraud.

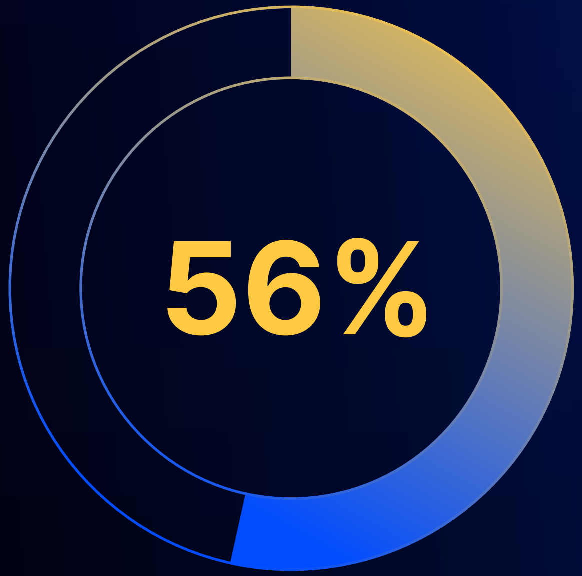
56% of organizations rely on double-check procedures to confirm financial reports are accurate, 47% on dual approval processes on payments, and 40% on segregation of duties. These measures are useful but far from sufficient seeing the level of sophistication reached by fraudsters. 5% don't have any defenses currently in place.

> I think fraud will increase because we're not paying enough attention. And until we take it seriously, implement systems, and do everything we can to prevent fraud, it will increase. To be in a world with less fraud, it's going to take concerted efforts from all companies, from all payment providers, and from anyone who's dealing with sensitive information.

Lee-Ann Perkins
Assistant Treasurer
Nacha Advisory Board member

#5 Corporates aren't sufficiently prepared for cyber-fraud

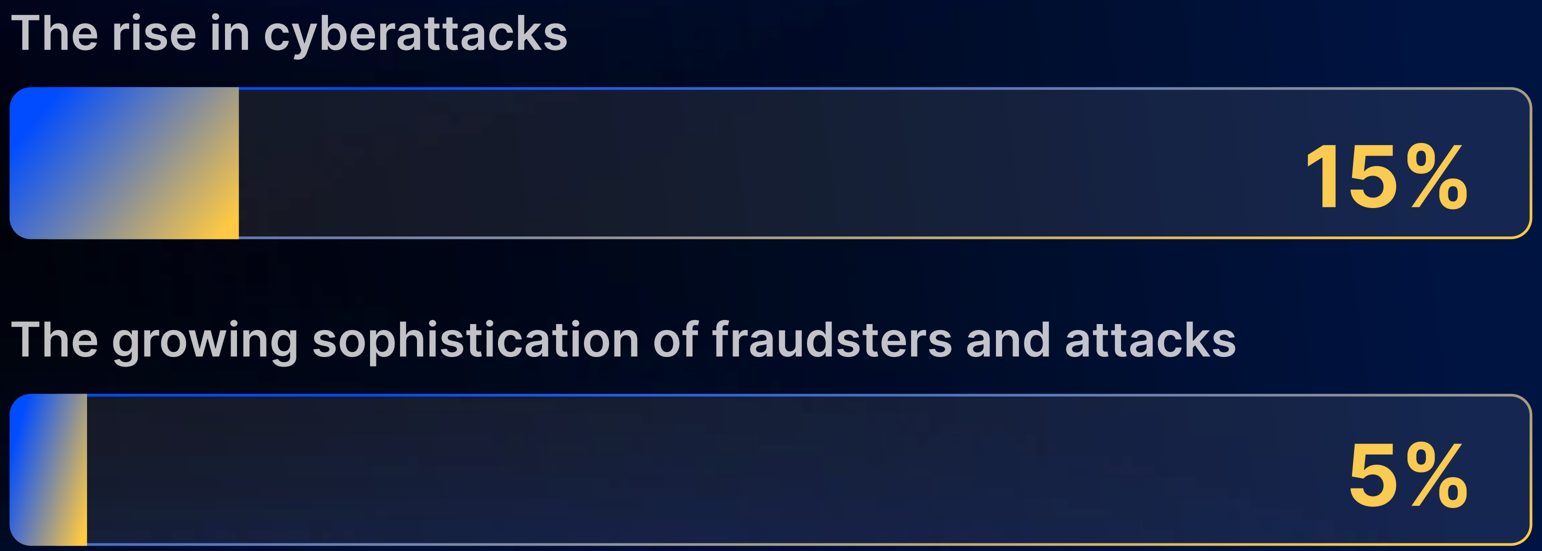
[1]



of companies have seen fraud prevention technology **budget increase in the last 6-12 months**

[2]

A **minority of companies** think one of the top challenges in fraud prevention is:



1- Has your budget for fraud prevention technology changed over the past 6-12 months? Respondents: 266
2- What is your biggest challenge when it comes to fraud prevention? Pick your top three. Respondents: 266

ANALYSIS

Fraud is happening more often, with **drastic consequences**. Yet, companies aren't sufficiently prepared to face it. 56% of companies have seen their fraud technology budget increase in the last 6-12 months. While this shows awareness, it can't top the 71% increase of targeted companies vs 2022. The paradox continues: 66% of companies expect fraud to keep increasing. This means some companies expect a continuing increase in fraud attempts, yet aren't allocating budgets to fight back.

This lack of budget can be explained by the **global shift to digitalization**. More tools are required across different teams and budget isn't prioritized for all teams. Fraud is often still seen as a Treasury problem only when it should be seen as a transverse issue that involves different departments. Indeed, it can happen at different stages of the P2P process, which involves many different teams.

What's even more surprising is that only 15% of companies think the rise in cyberattacks is a one of the top challenges to wiping out fraud, and only 5% think the growing sophistication of fraudsters and attacks is a top challenge to fraud prevention. Once again a paradox, considering the proportion of organizations (83%) that were targeted by cyber fraud in 2023.

> We hear about it, we go to conferences and we know it's happening. But I haven't seen with my own eyes enough seriousness in companies. It's happening and it could potentially be disastrous for companies, but not many take it seriously enough.

Lee-Ann Perkins
Assistant Treasurer
Nacha Advisory Board member

#6 From human only to automation first

[1]

42%

of companies say better training and education around payment fraud risks and cybersecurity risks are the most valuable strategies to fight fraud

[2]

40%

of companies have invested in fraud training

[3]

80%

have invested in cybersecurity training

[4]

49%

of companies say their biggest challenge in fighting payment fraud is that employees don’t always follow fraud prevention policies

1- Which of the following would be most beneficial in helping you minimize payment fraud in the next 12 months? Pick your top two. Respondents: 266
2- What defense measures do you have in place to fight payment fraud? Select all that apply. Respondents: 266
3- Has your organization given formal training on how to detect or prevent cyber fraud schemes? Respondents: 266
4- What is your biggest challenge when it comes to fraud prevention? Pick your top three. Respondents: 266

ANALYSIS

Training and education around fraud and cybersecurity (42%) are still seen as top defense measures to fight fraud at 43% of companies. Companies have put this in action over the last 12 months: 40% have invested in fraud training and 80% in cybersecurity training.

However, the biggest challenge that companies see in wiping out fraud (for 49% of organizations) is employees not following fraud prevention policies. A paradox emerges: companies favor employee training and rely on humans to fight fraud but think employees not following policies and training will be the main challenge in wiping it out.

While training is useful and mandatory to keep staff informed about the types of fraud they might be targeted by, it can't replace prevention tools. For budget and prioritization reasons, as well as a lack of awareness about market solutions, **companies aren't shifting to automation quickly enough** and are still lagging behind fraudsters.

> Training is useful, but it's nowhere close to sufficient to fight fraud, especially in this digital context. For me, the real issue is the lack of awareness of what exists on the market. Companies usually know fraud is an existing risk: they just don't know what exists to protect themselves against it.

Baptiste Collot
Co-Founder and CEO
Trustpair

#7 Automation, the key to fighting fraud

[1]

35%

of companies primarily use **human callbacks** for account validation

29%

... use **manual emails.**

[2]

The **top perceived challenges** in fraud prevention are:

Employees not following policies **49%**

Siloed processes blocking collaboration **48%**

Unreliable third-party data **36%**

[3]

For companies the **most beneficial measures** against fraud are:

Better education around fraud **43%**

Better education around cyber-risks **42%**

Increasing automation for prevention **38%**

1- How do you primarily handle vendor bank account validation? Respondents: 266
2- What is your biggest challenge when it comes to fraud prevention? Pick your top three. Respondents: 266
3- Which of the following would be most beneficial in helping you minimize payment fraud in the next 12 months? Pick your top two. Respondents: 266

ANALYSIS

Automation is the ultimate defense against fraud - especially cyber fraud. The only way to be sure you're paying the right person and bank account every time- and not a fraudster - is through data reliability. **Automated account validation guarantees data reliability** thanks to continuous checks throughout the payment chain. Even if fraudsters hack into your vendor's system and change the credentials, if you are constantly checking the credentials and data, you will catch a fraudster before sending them a payment. Software instantly detects the banking information is unknown and raises the alarm.

Unfortunately, 35% of companies primarily use human callbacks for account validation, and 29% use manual emails. Human callbacks and manual emails are fallible and error-prone, on top of being incredibly time-consuming, especially for companies working with thousands of vendors. These account validation methods aren't a match for sophisticated fraudsters hacking into company systems. On top of that, only 42% of organizations check banking information at various moments during the payment cycle: most of them stick to well-known checkpoints like onboarding (42%) or when a new invoice is submitted (57%), which means there are several moments where fraud can occur and organizations are vulnerable.

The good news is that companies seem to be aware their protection measures are insufficient and they need to rely more on automation. 38% say manual account validations are one of their top three challenges when it comes to fraud prevention, which indicates a clear need for automation. The same proportion says increasing automation will be the most beneficial to reducing fraud in their organization.

> “Companies have to use technology that's out there to help them. These AI-backed tools are the true answer to fight this war against fraud. They're the way to detect anomalies, intrusions, and so on. You can't fight the war with manual processes only”

Lee-Ann Perkins
Assistant Treasurer
Nacha Advisory Board member

In 2023, the landscape of payment fraud has drastically shifted to the cyber realm, profoundly impacting businesses. This surge in sophisticated fraud attacks has led to significant financial and reputational damages for companies. The response to this evolving threat, however, remains insufficient. Thankfully, some companies have embraced the risk and are raising budgets and defenses. However, there's still a notable gap in the adoption of advanced fraud prevention strategies. For businesses, 2024 will be the year to embrace more proactive and automated security measures.

> "Fraud is now completely in the digital era. We've seen the shift from manual to digital fraud: and now it's done. Fraud is an industry. A mature and equipped industry, with specialized fraudster organizations."

Baptiste Collot
Co-Founder and CEO
Trustpair

trustpair

Secure B2B payment, goodbye fraud.

Trustpair is the leading payment fraud prevention platform.

With the platform, more than 250 companies worldwide have already wiped out fraud.

Talk to an expert