



Exclusive Report

US Companies and B2B Payment Fraud

2023

Survey by **TREASURY & RISK**
THE FUTURE OF FINANCE TODAY



Editorial

In 2022, 56% of US companies were targeted by at least 1 fraud attempt. 12% were targeted by at least 10. These record-breaking numbers prove it: B2B payment fraud should be taken seriously.

The good news is that companies seem to understand the risk is real. In fact, 82% of senior leaders consider fraud prevention to be a top priority for 2023 and many projects are already underway.

Considering the right options to prevent B2B payment fraud

This report shows that organizations still rely very much on manual methods: 70% of companies still use phone calls to check supplier credentials changes. This a true paradox, considering that 55% of successful fraud attempts are perpetrated through credential or information changes on legitimate payments.

Considering the evolving nature of payment fraud, manual account validation is far from efficient. At GIACT and Trustpair, we can observe that frauds are more and more sophisticated and associated with cyber-attacks and social engineering.

A “humans only” policy just won’t cut it anymore when it comes to preventing B2B payment fraud.

Technology is key but it isn’t about replacing all human actions: it’s about using technology to make teams more efficient and focused on high-value tasks.

Training and educating teams about fraud is a big priority for US companies: 60% consider it the best approach to minimize fraud in the next 12 months. And while training is indeed necessary for all companies, it’s not self-sufficient and should be associated with the right tools.

Technology as a fraud shield

56% of companies think fraud attempts will increase in 2023. Thankfully, there are several technologies that they are already using to reduce the risk of fraud: the most common being controls built into ERP platforms.

It’s our responsibility as fraud experts to help companies continue their transition to technology, building secure processes and systematic account validation to prevent fraud.

With the expert insights of:



Baptiste Collot

CEO



Ramesh Menon

Group Director, Product Management, Digital Identity & Fraud Solutions



This report is based on a survey by:



Survey fielded between 2023-02-02 and 2023-03-02, 75 respondents

Table of contents

01

Insight 1

56% of US companies were affected by payment fraud in 2022

02

Insight 2

The impact of payment fraud goes further than financial losses

03

Insight 3

Companies still rely on manual and inefficient processes to prevent fraud

04

Insight 4

Fraud events are expected to increase in 2023, asking for adequate safeguard measures

01

Insight 1

**56% of US companies were
affected by payment fraud
in 2022**

Insight 1 56% of US companies were affected by payment fraud in 2022

Most US companies have been targeted by at least one fraud attempt in 2022

The risk of payment fraud is very real: in 2022, it affected almost 6 out of 10 companies in the US. Furthermore, most companies that were a victim of fraud attempts were targeted more than once. 12% of all US companies were targeted more than 10 times and 5% more than 15 times.

These record-breaking numbers can be linked to **changes in the way fraudsters operate**: more sophisticated, organized, and specialized – the threats aren't the same as they were 10 years ago.

How many incidents of payment fraud has your organization fallen victim to in the past 12 months?



- 56%** have been targeted **at least once**
- 43%** have been targeted **more than once**
- 12%** have been targeted **more than 10 times**

We can definitely say that the pace of payment fraud isn't slowing down, quite the opposite. A decade ago, fraud was very manual: now it's sophisticated and complex. It should be a big concern for any company.

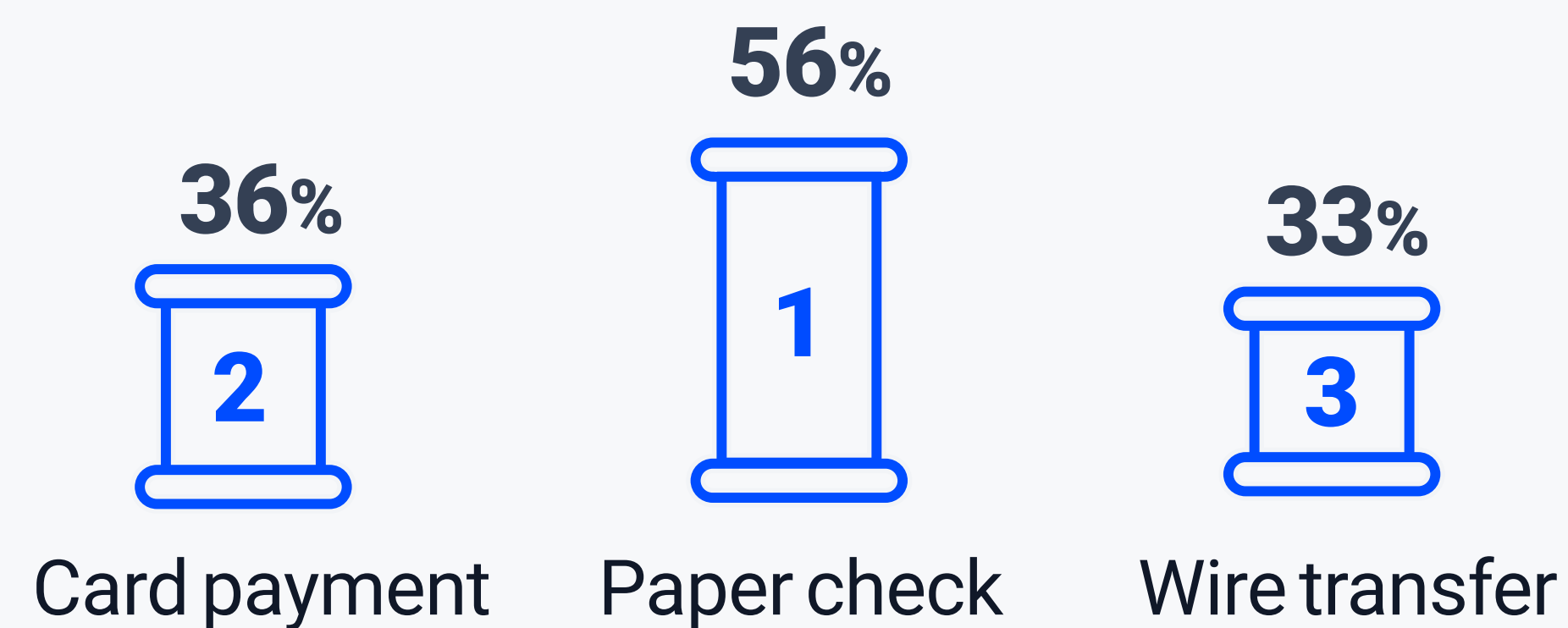
Baptiste Collot - Trustpair

Insight 1 56% of US companies were affected by payment fraud in 2022

The most common type of fraud was paper check fraud

Paper checks are still used by 40% of companies in the US, which can explain why it's still a very common type of fraud – the most common in fact. This is interesting given how time-consuming and inefficient paper checks can be, in addition to the security loopholes they can present.

What types of payment frauds were most successful?



It's no wonder check fraud is the most common type of payment fraud: it's very hard to fight! A digital alternative will make it easier to detect fraud and secure payments. The move to wire transfer or ACH would be legitimate, for security and productivity reasons.

Baptiste Collot - Trustpair

Fraud was most often perpetrated with credentials and information changes on legitimate payments

55% of companies targeted by fraud attempts indicated changes in supplier credentials on legitimate payment as the way the fraud was perpetrated. 33% indicated business email compromise and phishing.

This makes sense, considering paper checks and wire transfer fraud are among the most common types of fraud. These types of frauds are triggered by fraudulent changes to supplier credentials. The fraudsters might send an email impersonating a supplier and asking to change their bank account information for example.

This underlines the importance of **having solid supplier account validation processes.**

How was the fraud perpetrated?



55% Supplier information changed



33% Business email compromise

02

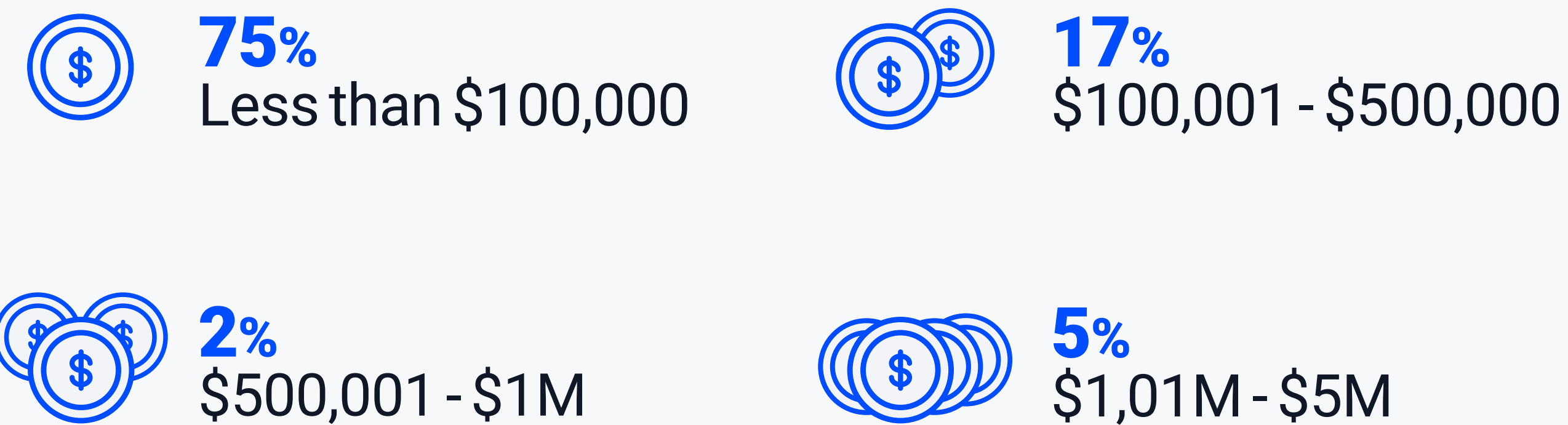
Insight 2

**The impact of payment
fraud goes further than
financial losses**

Insight 2 The impact of payment fraud goes further than financial losses

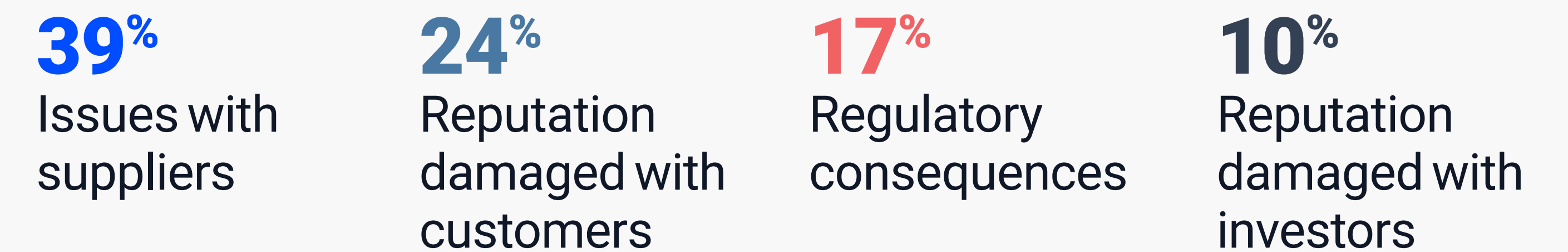
24% of companies victims of fraud lost more than \$100,000, and 5% lost more than \$1 million

What were the direct financial losses to your organization ?



For 39% of companies, fraud incidents also generated issues with suppliers

What were the other impacts of the incident(s)?



As seen above, **financial losses can be very extensive** when it comes to payment fraud. In fact, for 5% of US companies, losses crossed the \$1 million mark. For smaller businesses, this can have a long-lasting – or even dramatic – impact.

However, **financial losses aren't the only impact**. In fact, 39% of companies highlight issues with suppliers as a result of fraud. 24% indicated fraud damaged their organization's reputation with customers.

The impact on suppliers can be mistrust, damaged communications, or even real friction when the fraud isn't detected for some time and your supplier doesn't receive payment.

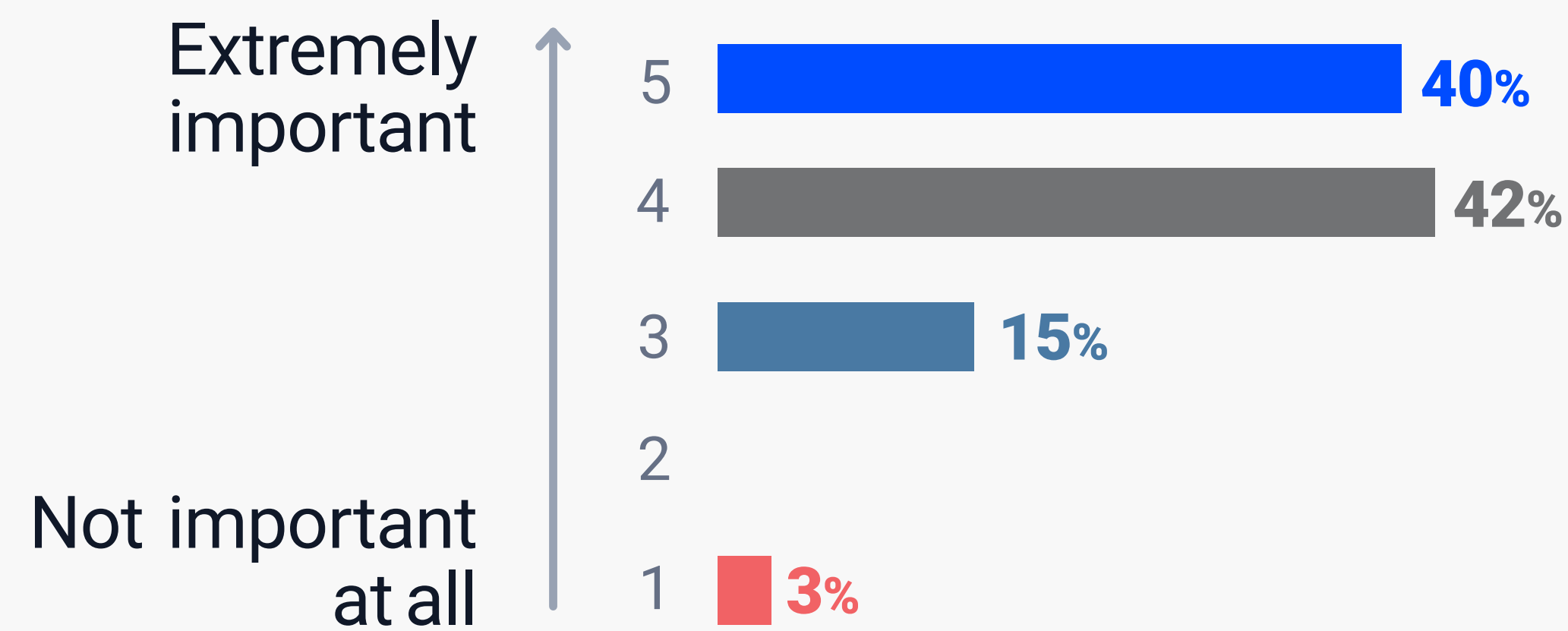
The first impact of fraud on your supplier is late payment. Your company hasn't paid its' actual supplier. The second impact is a reputational risk. The third impact would be friction to determine the responsibility for the fraud. Unfortunately, this can lead to legal actions in some cases.

Baptiste Collot - Trustpair

Insight 2 The impact of payment fraud goes further than financial losses

In response, 82% of company senior leaders consider fraud prevention to be an important priority

How would you rate the importance your organization's senior leadership places on payment fraud prevention?



Fraud prevention is a journey everybody's on. There's no destination or defined conclusion. Fraud is going to keep happening. Organizations need to approach this holistically, on a cross team level.

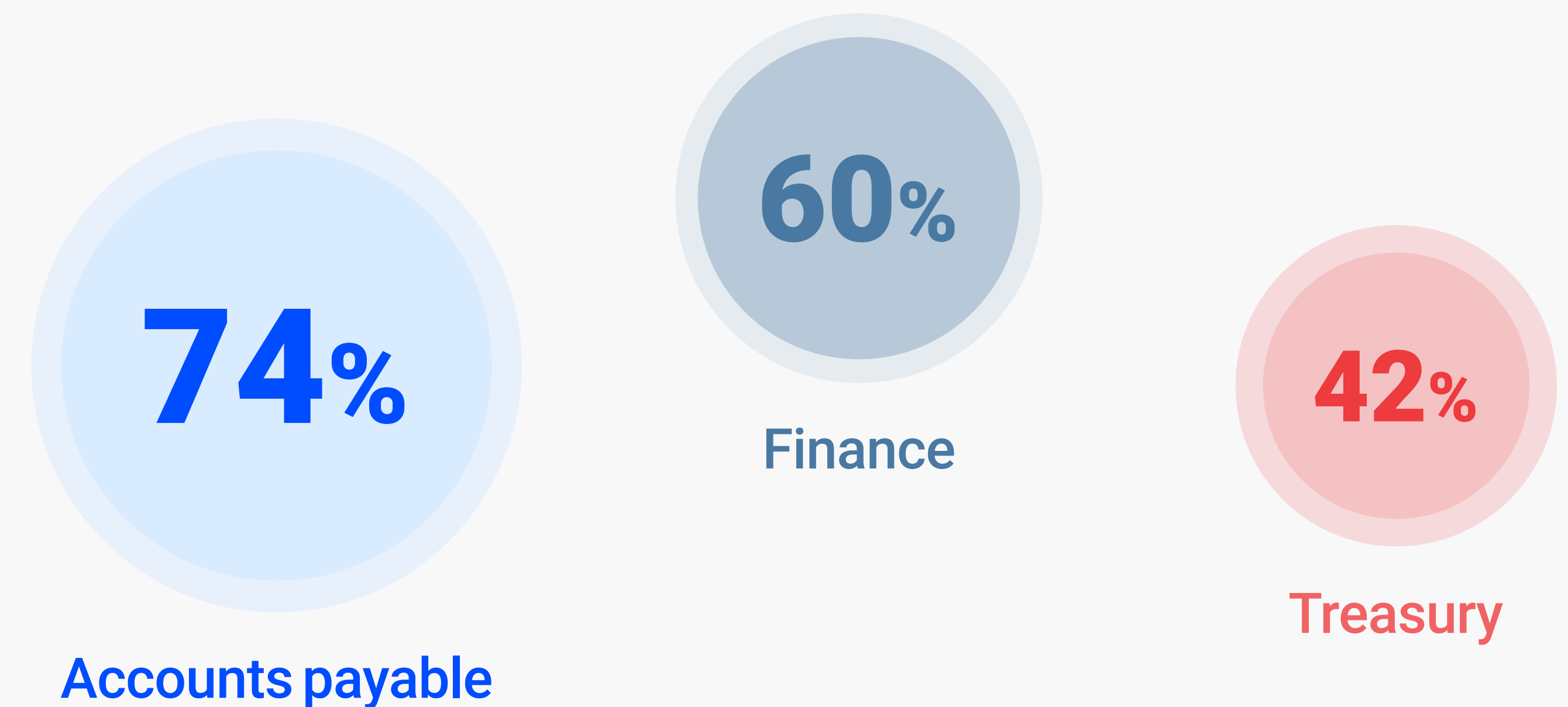
Ramesh Menon - GIACT

And the fight against fraud concerns many different corporate functions within organizations

74% of companies consider A/Ps as the most critical corporate function to mitigate the risk of payment fraud, 60% indicated Treasury, and 42% Finance.

Fraud is a cross-team priority because it can spread out during the whole payment chain and have an impact on all layers of the company. That's why it's critical to set up **fraud prevention measures throughout the whole P2P process** and not only at specific moments of the payment chain.

Which are the most critical corporate functions for mitigating the risk of payment fraud?



03

Insight 3

**Companies still rely on manual
and inefficient processes to
prevent fraud**

Insight 3 Companies still rely on manual and inefficient processes to prevent fraud

Companies have set up many policies in the last year to help reduce fraud

What policies and procedures have you added in the past 12 months to reduce the risk of payment fraud?

Changed payment process (53%)

Added manual review for changes to payment instructions (37%)

Changed payment systems log in authentication (33%)

Eliminated payments bypassing standard process (23%)

Other (13%)


Required multifactor authentication (36%)

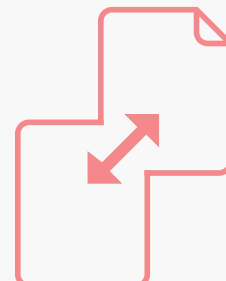
Reduced usage of paper checks (27%)

More frequent account verifications (19%)

But these processes are still very manual: 70% of companies use human callback as a validation procedure to verify changes to supplier credentials

What validation procedures do you use to verify changes to supplier account information?

70%
 Human callback

59%
 Internal segregation of duties in validation

14%
 Double signature from supplier management

4%
 Other

Companies are setting up many policies. In fact, 53% have changed their internal payment initiation and approval processes. However most companies – 70% – use human callback to verify changes to supplier account information. This manual process is **very time-consuming**, especially for larger companies that have thousands of suppliers. It also means having someone dedicated to this job only.

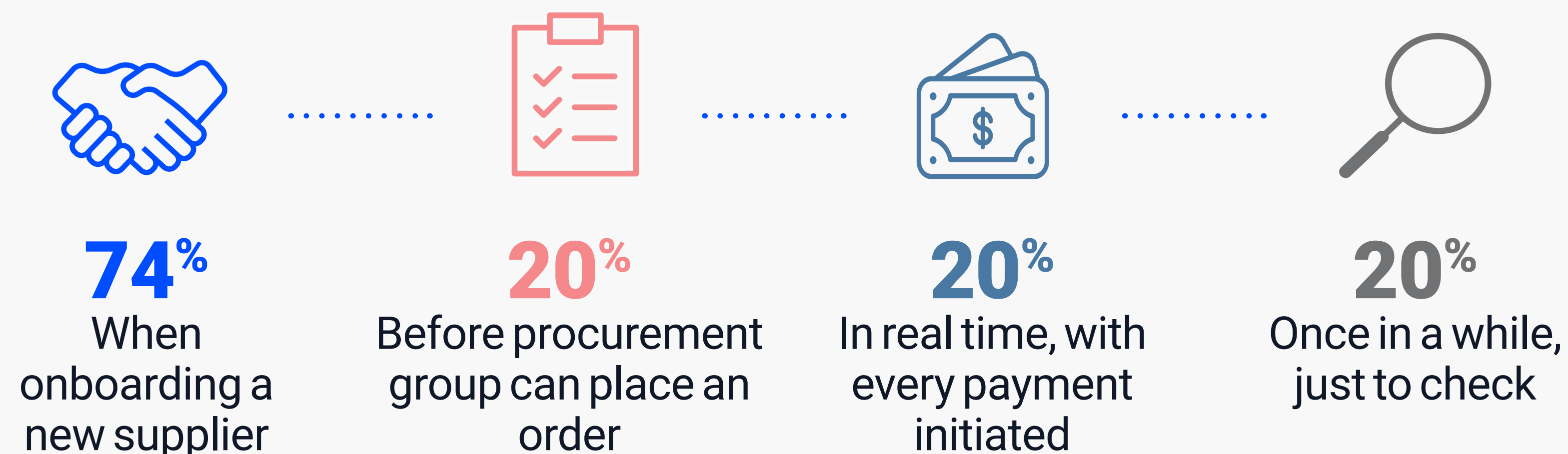
Insight 3 Companies still rely on manual and inefficient processes to prevent fraud

Account validation is still associated with specific moments of the supplier relationship

A lot of attention is paid before letting someone in the door, but not enough throughout the rest of the supplier lifecycle. Ideally, any type of interaction means reverifying your supplier's information.

Ramesh Menon - GIACT

When does your organization require account validation for a supplier?



74% of companies do account validation checks when onboarding a new supplier. This proportion drops dramatically when it comes to checks at other moments of the supplier relationship: **only 20% of companies control supplier information before placing an order, before payment campaigns, or once in a while just to check.**

This a true paradox, considering that 55% of successful fraud attempts are perpetrated through credential or information changes on legitimate payments. **Controls on supplier credentials should be a priority** during the whole supplier relationship and especially before payment campaigns.

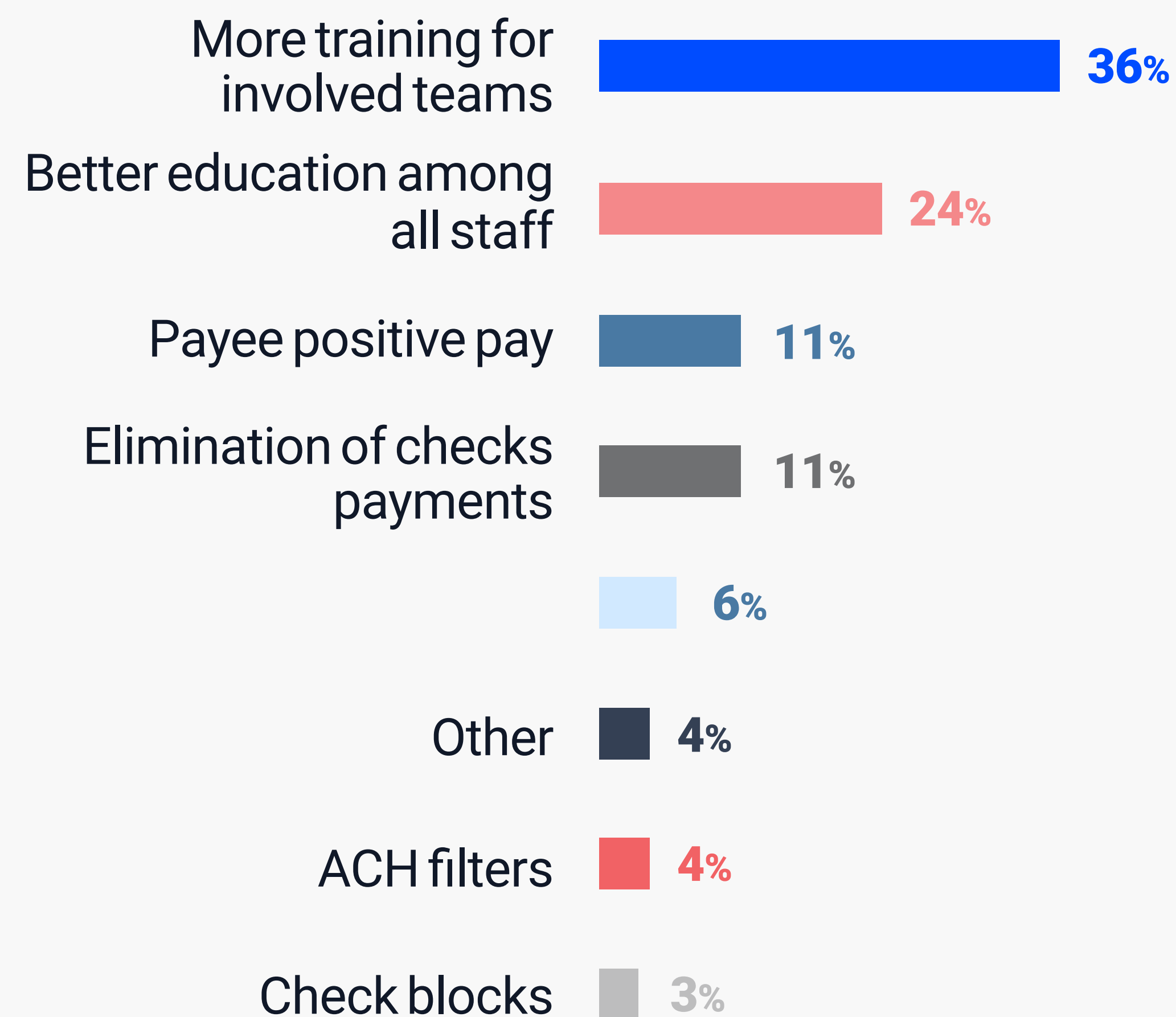
Companies have to completely change the way they secure their P2P process, making it less manual and more efficient. They need to cover all the P2P process: controls on supplier data should be led continuously, not only when onboarding a supplier. This concerns all teams, from Procurement to AP teams or even the Treasury department.

Baptiste Collot - Trustpair

Insight 3 Companies still rely on manual and inefficient processes to prevent fraud

60% of companies see training and better education as their primary approach to minimizing fraud

What do you see as the most effective approach to minimize payment fraud in the next 12 months?



Fraud prevention training is a big priority for US companies. In fact, 36% consider more training for teams involved in initiating and approving payments as the best approach to minimize fraud in the next 12 months. 24% indicated better education among managers and staff.

On the whole, **60% of companies see training and better education as their primary method to reduce fraud**. This proportion is far more important than other approaches like switching off paper checks companywide (11%) or resorting to automated supplier account validation (6%).

While training is important for companies, it's insufficient and should be associated with the right tools. Cyber-attacks are best managed with a multi-pronged approach.

Training is not optional: companies will always need better education. But training isn't self-sufficient. It needs to be associated with the right tools and technology. Education and tools are complementary: they're both lines of defense against fraud, stronger together than alone.

Baptiste Collot - Trustpair

04

Insight 4

Fraud events are expected to increase in 2023, asking for adequate safeguard measures

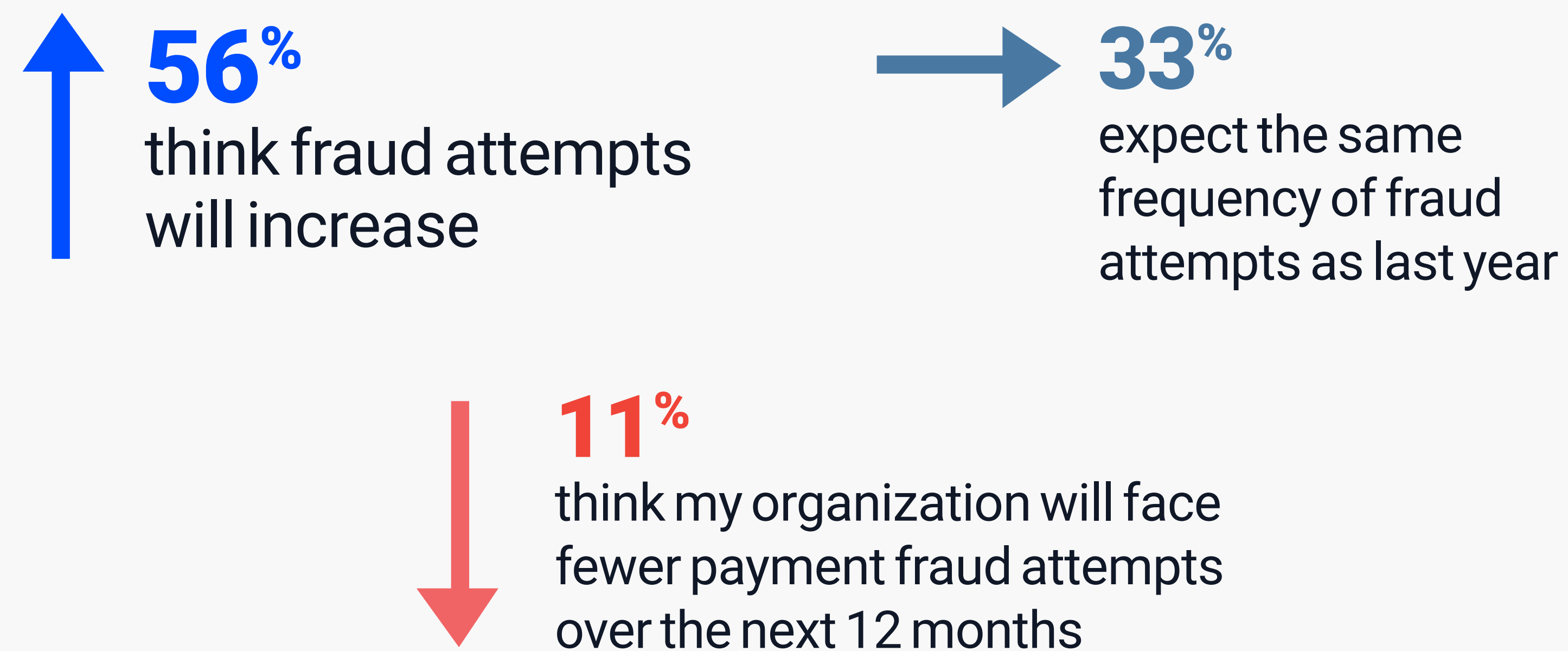
Insight 4 Fraud events are expected to increase in 2023, asking for adequate safeguard measures

More than 1 company out of 2 thinks payment fraud attempts will increase over the next 12 months

Only 11% of US companies think they will face fewer fraud attempts in 2023. For the most part, **organizations think fraud events will increase**. 20% of companies think they will even increase substantially over the next 12 months.

This is unsurprising, given the risky economic and geopolitical climate we're in – a climate in which fraudsters are developing ever more sophisticated techniques.

Do you expect payment fraud attempts to increase over the next 12 months?



The pandemic accelerated the shift to digital for everyone, including fraudsters!

With fraudsters using ever more sophisticated techniques, our industry needs to raise awareness of existing and new threats as they arise. The answer is automation. What automation can do for you is better than what your best employees can do. Automation raises standards and supports decision-making.

Ramesh Menon - GIACT

Insight 4 Fraud events are expected to increase in 2023, asking for adequate safeguard measures

43% of companies see the sophistication of BEC and social engineering attacks as the main obstacle to eliminating fraud

Companies expect **fraud events to increase in 2023**. And whilst they're setting up security measures to fight off these attempts, they also identify specific obstacles to watch out for in their fight against fraud.

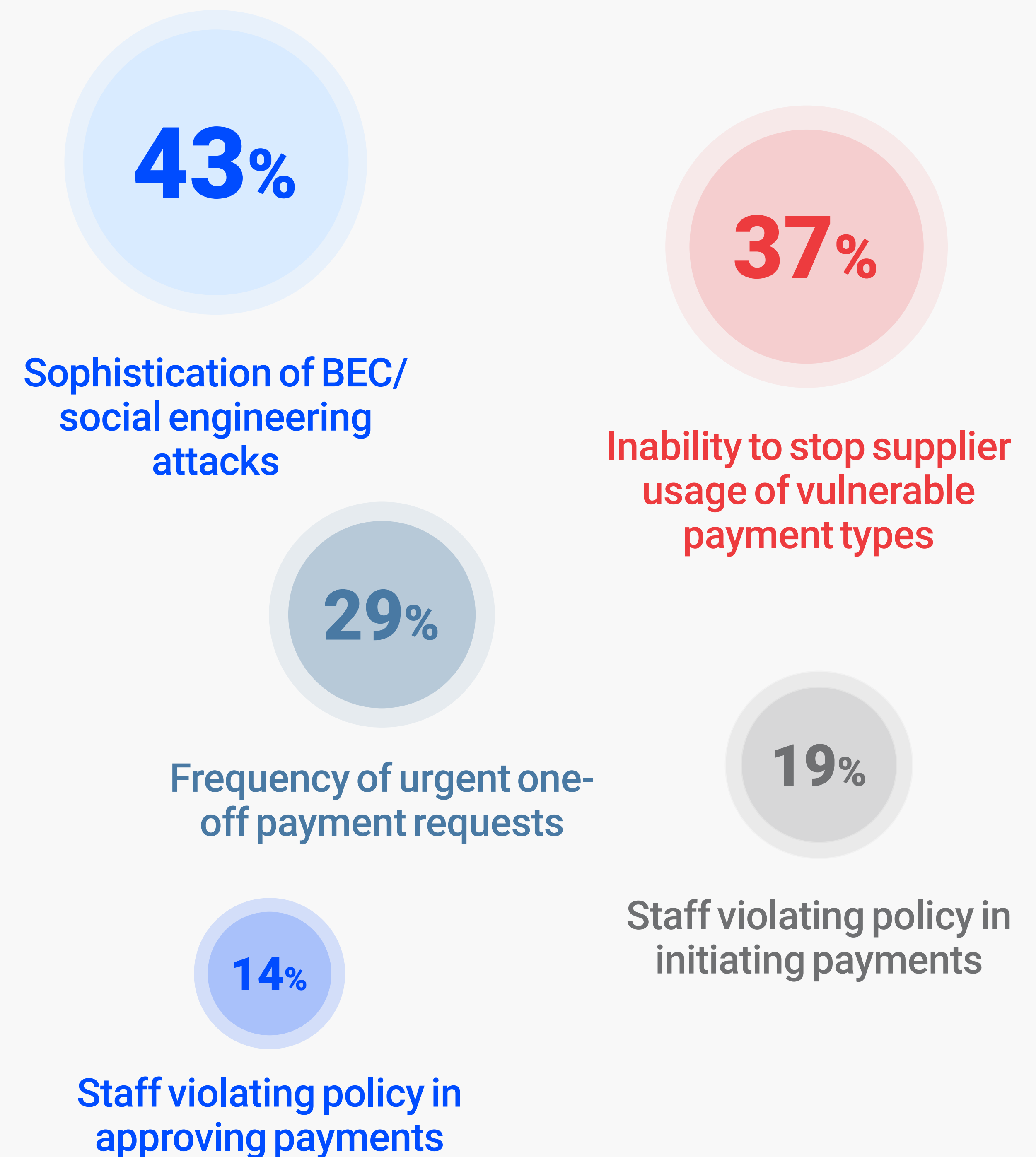
43% of companies see the sophistication of BEC and social engineering attackers as the main obstacle: this shows **awareness regarding the evolution of fraud** itself. However, it's also quite a paradox compared to the proportion of companies that think training will be their primary approach to resolving fraud.

37% of companies identify their inability to wean suppliers off of more-vulnerable payment types as the main blocker: this can be linked to **the widespread use of paper checks in the US**.

It's a huge paradox to see that companies are aware that fraud is getting more and more sophisticated and see this complexity as a major blocker in their fight against fraud but still think they'll be able to stop fraud with training only. You can't fight cyber-attacks with a 'human only' policy

Baptiste Collot - Trustpair

What are your organization's key stumbling blocks to eliminating the risk of payment fraud?



Insight 4 Fraud events are expected to increase in 2023, asking for adequate safeguard measures

Thankfully, 54% of companies already use their ERP or TMS to control the risk of fraud

What technologies are you using to reduce the risk of payment fraud?

- ✓ **54%** - Controls built into ERP or TMS platform
- ✓ **50%** - Payee positive pay
- ✓ **47%** - ACH filters
- ✓ **40%** - User-authentication and cybersecurity tools
- ✓ **26%** - Check blocks
- ✓ **17%** - Automated supplier account validation systems
- ✓ **3%** - Other

Companies already **use several technologies to control fraud risk**: 54% use controls built into their ERP or TMS, 50% use payee-positive pay, and 47% use ACH filters.

Controls integrated into ERP and TMS software offer the most efficient way of fighting payment fraud. They're automated and save hours of manual work, enabling finance teams to **focus on where the risk really is**.

I think human and technology are complementary. Technology should be used to enhance human actions and not replace them. People get better at their jobs thanks to technology. Technology will help you focus on where your risk really is.

Baptiste Collot - Trustpair

To sum up

Ultimately, we need to rely on systems. We need to rely on data, analytics, and clear insights. All that in a completely automated fashion that will help human beings make the right decisions.

Ramesh Menon - GIACT

Payment fraud is a **growing concern for financial professionals**, with over half of US companies reporting that they have been victims of a fraud attempt in 2022. Almost one in three (30%) said the number of incidents has increased year-over-year. Moreover, 56% of organizations expect to see an increase in fraud attempts in 2023.

The **most common payment fraud in 2022 was paper checks**, followed by card payments and wire transfers. This can be linked to the widespread use of paper checks in the US. More than 1 out of 2 companies victims of fraud in the past year said the method of attack **involved changing supplier credentials and/or information on legitimate payments**.

Thankfully, the problem is being taken seriously by senior leadership, with 82% reporting that fraud prevention is an important priority. Moreover, **responsibility for preventing fraud is a team effort** with several departments playing their part.

Overall, companies have put in place a wide variety of fraud-combatting policies and procedures like changing internal payment initiation and approval processes or adding a manual review for payment change requests.

However, **most processes are still manual**: especially when it comes to controlling supplier credentials and information. These manual processes do not seem sufficient to fight fraud, especially considering the evolving nature of fraud. Companies themselves point to the high level of sophistication of BEC and social engineering as the main blocker to minimize fraud.

Companies also **rely heavily on training and better education** as the way forward. 36% of companies expect more training for procurement, accounts payable, and finance teams and 24% see better training for staff and management.

Training is of course important, but it's not enough. Companies need to rely more on technology to fight fraud. Fraud prevention software will help finance teams focus on where the risk really is and reduce low-value tasks. The good news is that **54% of companies already use their ERP or TMS to control the risk of fraud**.

These integrated controls are the future of fraud prevention. And it's our responsibility as fraud experts to support companies along the digital transition.

Methodology

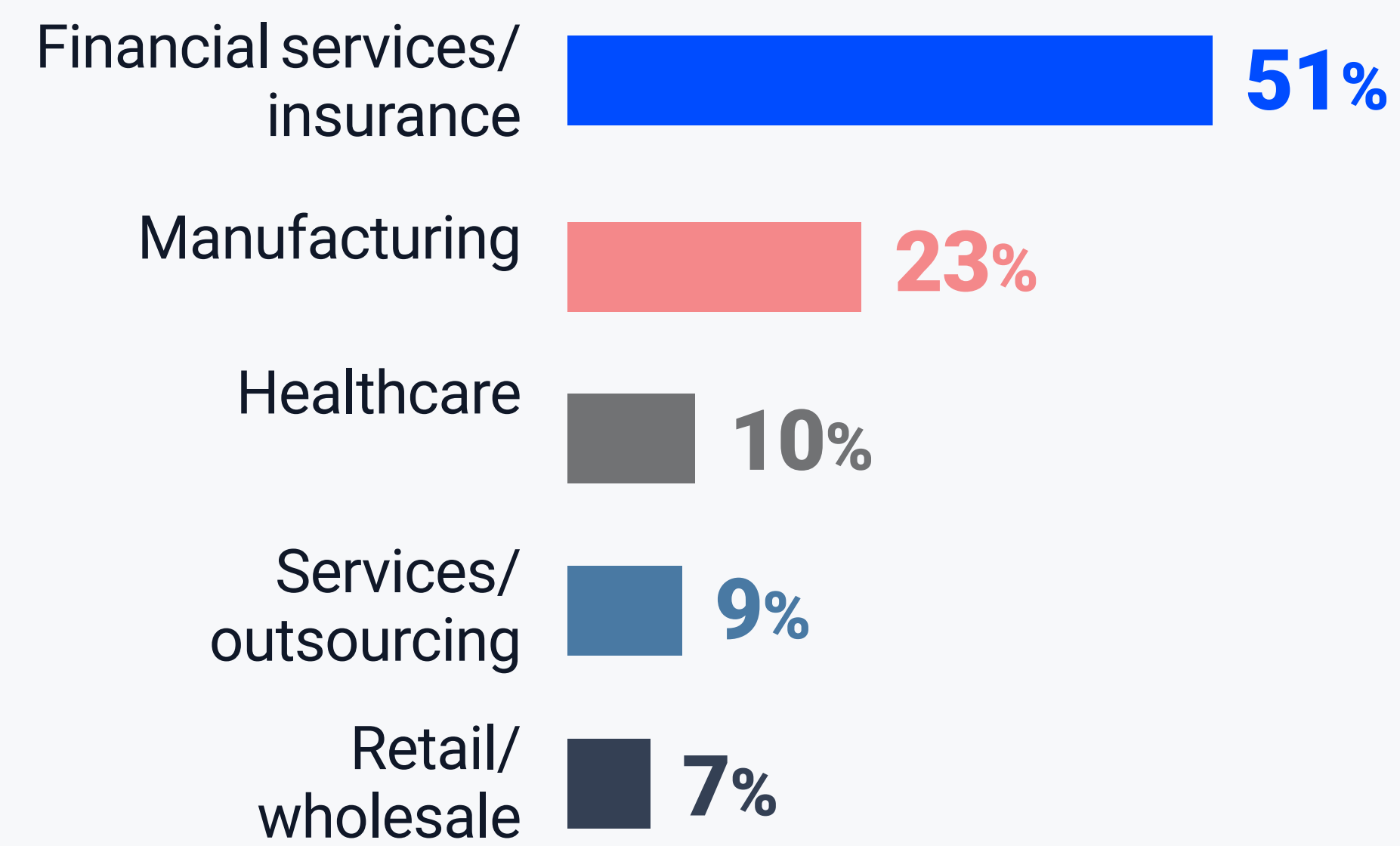
Survey carried out by Treasury and Risk for Trustpair and GIACT.

This survey was fielded via email to Treasury & Risk's universe of treasury professionals.

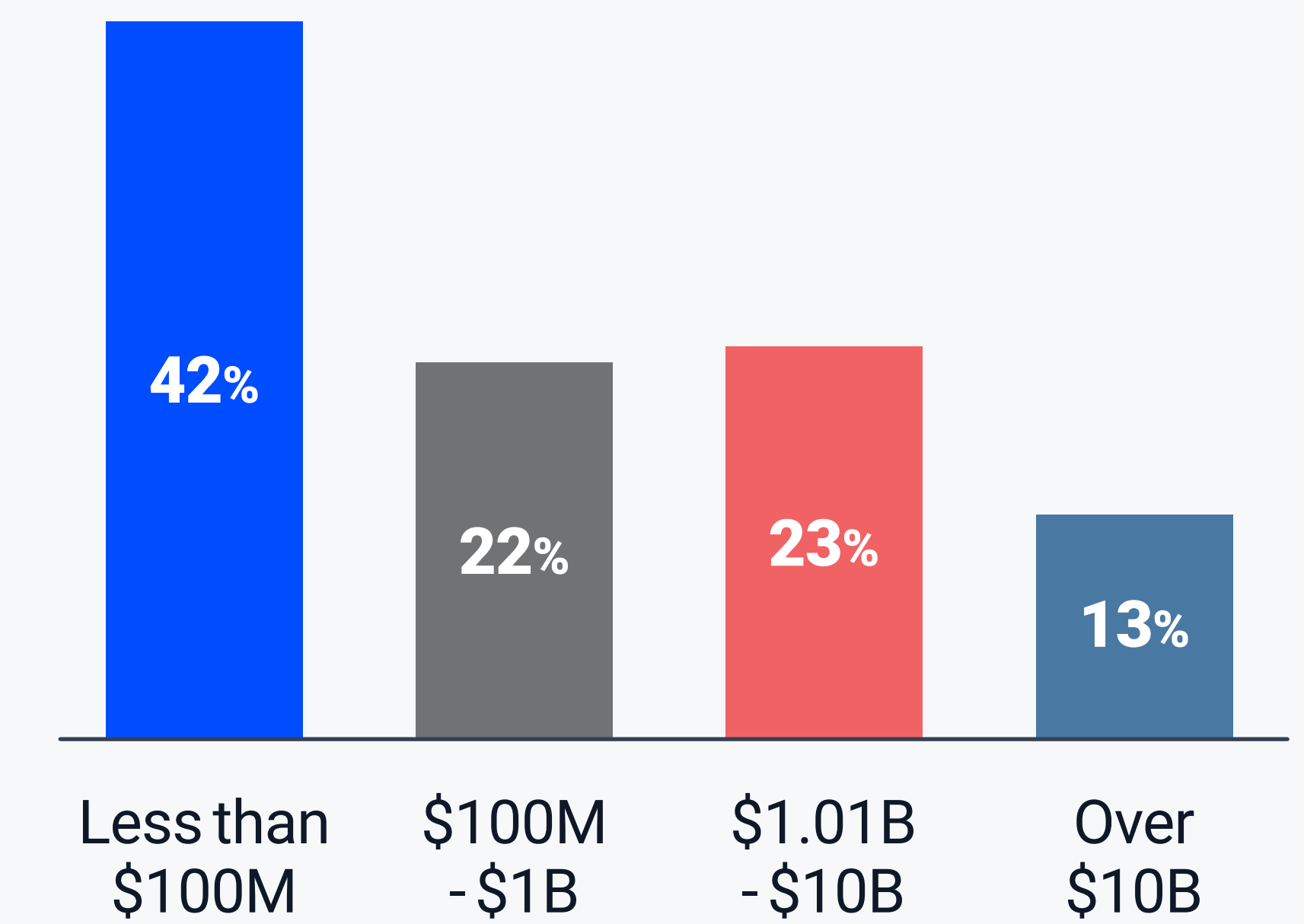
In-field dates: February 2, 2023, through March 2, 2023.

Total number of survey respondents: 75

Respondent Business Sector



Respondent Company Revenue



Respondent Job Title

Job title	%
Treasury Manager	27%
CFO	24%
Treasury Team	12%
Operational manager	10%
SVP/EVP/VP/director finance	9%
Other	9%
Financial analyst/other finance	6%
A/P manager/director	3%

Our partners

This **2023 B2B Payment Fraud report** was commissioned by:



[Learn More](#)



[Learn More](#)



[Learn More](#)



Secure B2B payment, goodbye fraud.

Trustpair is the leading payment fraud prevention platform for large companies worldwide.

Get expert advice

Available on
SAP Store

