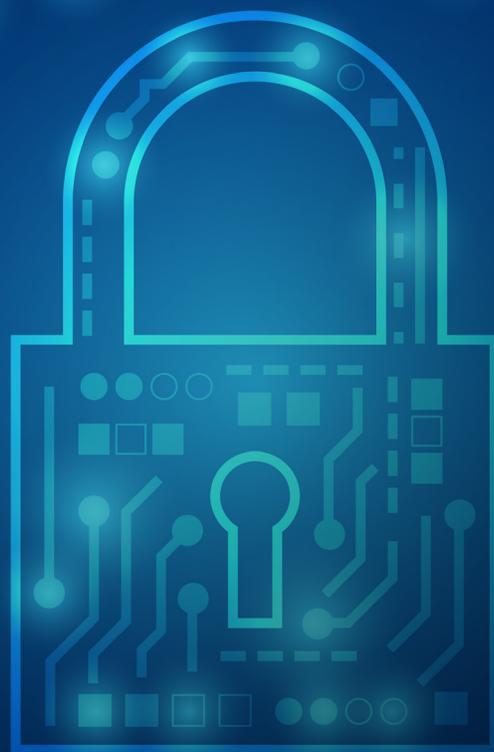


The Real Cost of Online Fraud

Ponemon
INSTITUTE

Sponsored by PayPal



Contents

Introduction	03
Key Findings	
Security of online transactions	05
Organizations' approach to securing online transactions	10
The risks of digital transformation to online security	14
COVID-19 and online fraud	15
The cost of fraud and budget	18
Best practices from organizations that are highly effective in investigating online fraud	20
Methods	24
Caveats	27

Introduction

The purpose of this research is to understand the current fraud landscape, barriers and challenges organizations face in mitigating the risk of online fraud and the resulting financial losses. The findings reveal that the number one challenge is the increasing sophistication of fraudsters followed by not having the right technologies to mitigate online financial fraud.

Sponsored by PayPal, Ponemon Institute surveyed 632 individuals who are familiar with their organizations' efforts to prevent fraud and are involved in fraud investigation and mitigation and/or cybersecurity activities.

Sixty-one percent of respondents hold supervisory positions or higher in their organizations. Most of these respondents' industry focus is eCommerce (27 percent), merchants (21 percent), retailers (16 percent) and travel (10 percent). A complete breakdown of industries represented in this research is presented in the Appendix of this report. Many of these respondents admit their organizations' current tools or practices are not very

effective in investigating online fraud and achieving compliance with IT security and privacy regulations.

Another key takeaway from this research is that **COVID-19 is seriously affecting organizations' ability to protect online financial transactions against fraud.** Prior to COVID-19, 45 percent of respondents rated their effectiveness as high or very high. Today, only 34 percent of respondents rate their effectiveness as high or very high. Although digital transformation is important to organizations' ability to support business goals, it challenges their ability to prevent online fraud incidents.

According to the research, **organizations represented in this research are losing an average of \$4.5 million per year due to online fraudulent transactions.** As shown in Figure 1, despite these losses only slightly more than half (51 percent of respondents) say their organizations make it a priority to protect online financial transactions. Only 38 percent of respondents say the cost of protection outweighs the cost of dealing with losses.



Figure 1.
Perceptions about the protection of online financial transaction

Strongly agree and Agree responses combined

The following findings provide guidance on reducing online fraud risks.

- Prioritize the protection of online transaction by having the necessary in-house expertise, joined with industry partners to effectively process and secure transactions and regularly assess the ability of the IT system to prevent and contain online financial fraud. **Sixty-one percent of respondents say their organizations do not have the right technologies to mitigate online financial fraud.**
- To address the lack of in-house expertise, organizations need to rely upon tools and resources using machine learning. **Less than half of respondents say their organizations have the necessary in-house expertise to prevent and contain online fraud (45 percent of respondents).**
- Consider investing in machine learning and advanced analytics. The top benefit is better integration with threat intelligence sources. Sixty percent of respondents say such technologies are essential to detecting online fraud and 51 percent of respondents say their organizations use automation, machine learning and/or behavioral analytics fraud.
- To prevent chargeback fraud, organizations should have clear merchant descriptors, clear and flexible return policies and ensure every dispute is responded to.
- Be aware of how digital transformation can increase the risk of an online fraud attack. Seventy-nine percent of respondents are significantly concerned (30 percent), very concerned (31 percent) or concerned (18 percent) that digital transformation may increase the risk of a fraud attack. Address increasing vulnerabilities from digital transformation. **Eighty-one percent of respondents say their organizations are more vulnerable from digital transformation and should consider leveraging advanced intelligence in the payment processing process.**
- Take steps to decrease the time to detect, contain and respond to an online fraud incident. Thirty-eight percent of respondents say the time it takes to detect, contain and respond to an online fraud incident has increased.
- To create and retain trust in online transactions, organizations should have policies to ensure strict security safeguards are in place and inform customers what sensitive data is used in online financial transactions. The data that is considered most at risk and particularly needs to be safeguarded are financial information, customer information and payment data.
- Create a collaborative relationship between the fraud and cybersecurity teams to improve the detection and investigation of online fraud. While 64 percent of respondents say collaboration is very important, only 29 percent of respondents say collaboration is achieved.



Key Findings

This section features an analysis of the research findings. The complete audited findings are presented in the Appendix of this report. The following topics are covered in this report.



Security of online transactions



COVID-19 and online fraud



Organizations' approach to securing online transactions



The cost of fraud and budget



The risks of digital transformation to online security

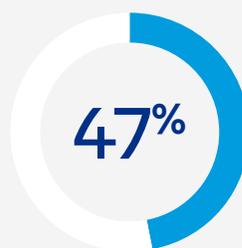


Best practices of organizations most effective in reducing online fraud



Security of Online Transactions

Not prioritizing the risk of online fraud creates barriers to achieving security. As shown in Figure 2, less than half of respondents say their organizations regularly assess the ability of its IT systems to prevent and contain online financial fraud (47 percent of respondents) and less than half have the necessary in-house expertise to prevent and contain online fraud (45 percent of respondents).



My organization regularly assesses the ability of its IT systems to prevent and contain online financial fraud



My organization has the necessary in-house expertise to prevent and contain online fraud

Figure 2.
Barriers to achieving fraud prevention
Strongly agree and Agree responses combined

Only about half of respondents (52 percent) say their organizations are very effective in reducing online fraud. Respondents were asked to rate the effectiveness of their ability to mitigate the consequences of online fraud on a scale from 1 = not effective to 10 = highly effective.

Figure 3 presents the very effective and highly effective responses (7+ responses on the 10-point scale). Only 45 percent of respondents say their organizations are very effective in investigating online fraud. Even more concerning is that only 35 percent of respondents say they are very effective in investigating online fraud and only 20 percent of respondents say they are very effective in preventing chargeback fraud.

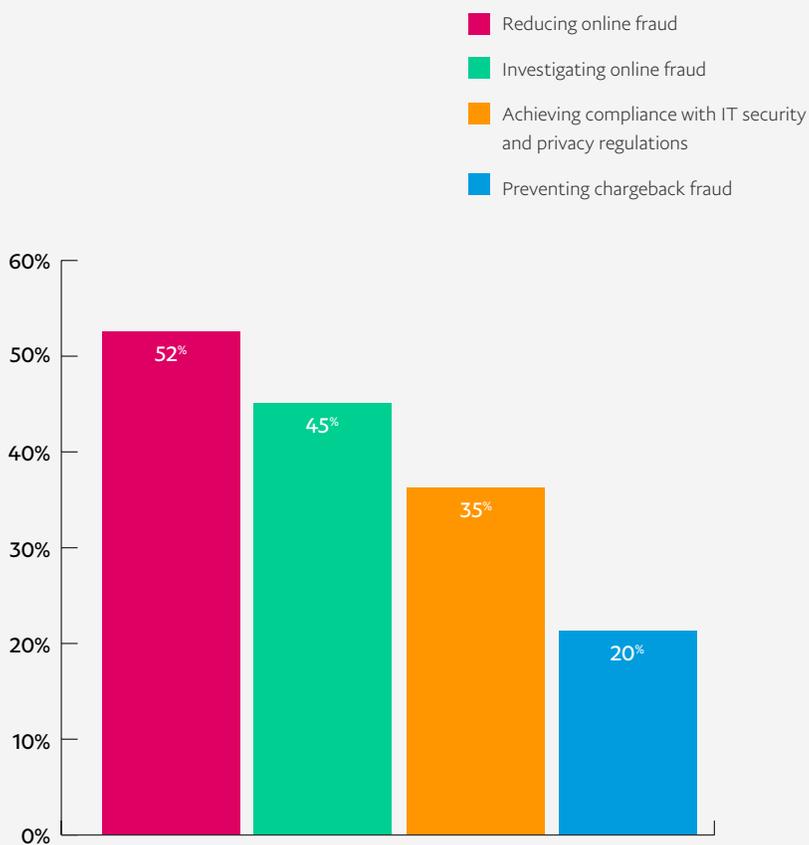


Figure 3.
Perceptions about the ability to mitigate the risks of online fraud

On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented





Not having the necessary in-house expertise and the right technologies make it difficult to deal with the increasing sophistication of fraudsters. Figure 4 presents the challenges organizations face in mitigating online financial fraud. As shown, **65 percent of respondents say the number one challenge is the increasing sophistication of fraudsters followed by 61 percent of respondents who say their organization does not have the right technologies to mitigate online financial fraud.**

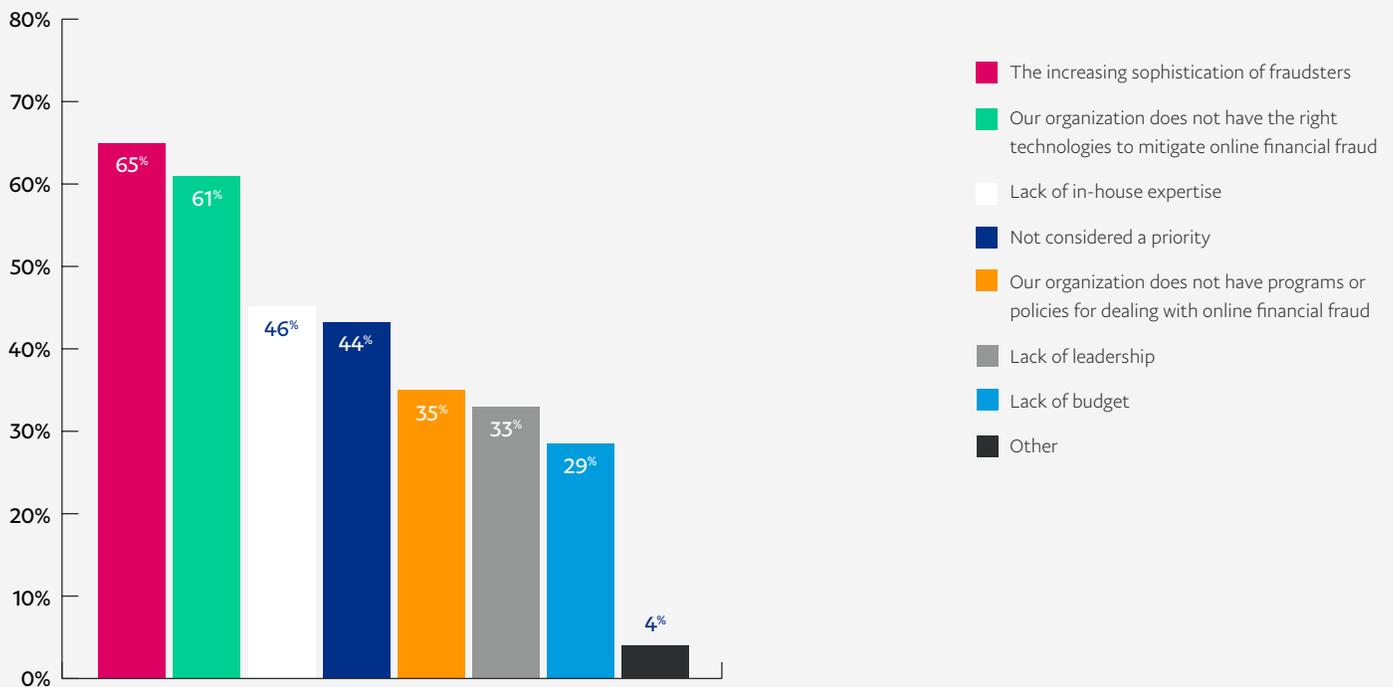


Figure 4.
Primary challenges to mitigating online financial fraud

More than one response permitted

Financial, customer and payment data are considered most at risk in online financial transactions.

Most respondents are in eCommerce (27 percent), merchants (21 percent), retailers (16 percent), travel (10 percent) and hospitality (9 percent). They are particularly sensitive to the risk to financial information (69 percent of respondents), customer information (68 percent of respondents) and payment data (63 percent of respondents), as shown in Figure 5.

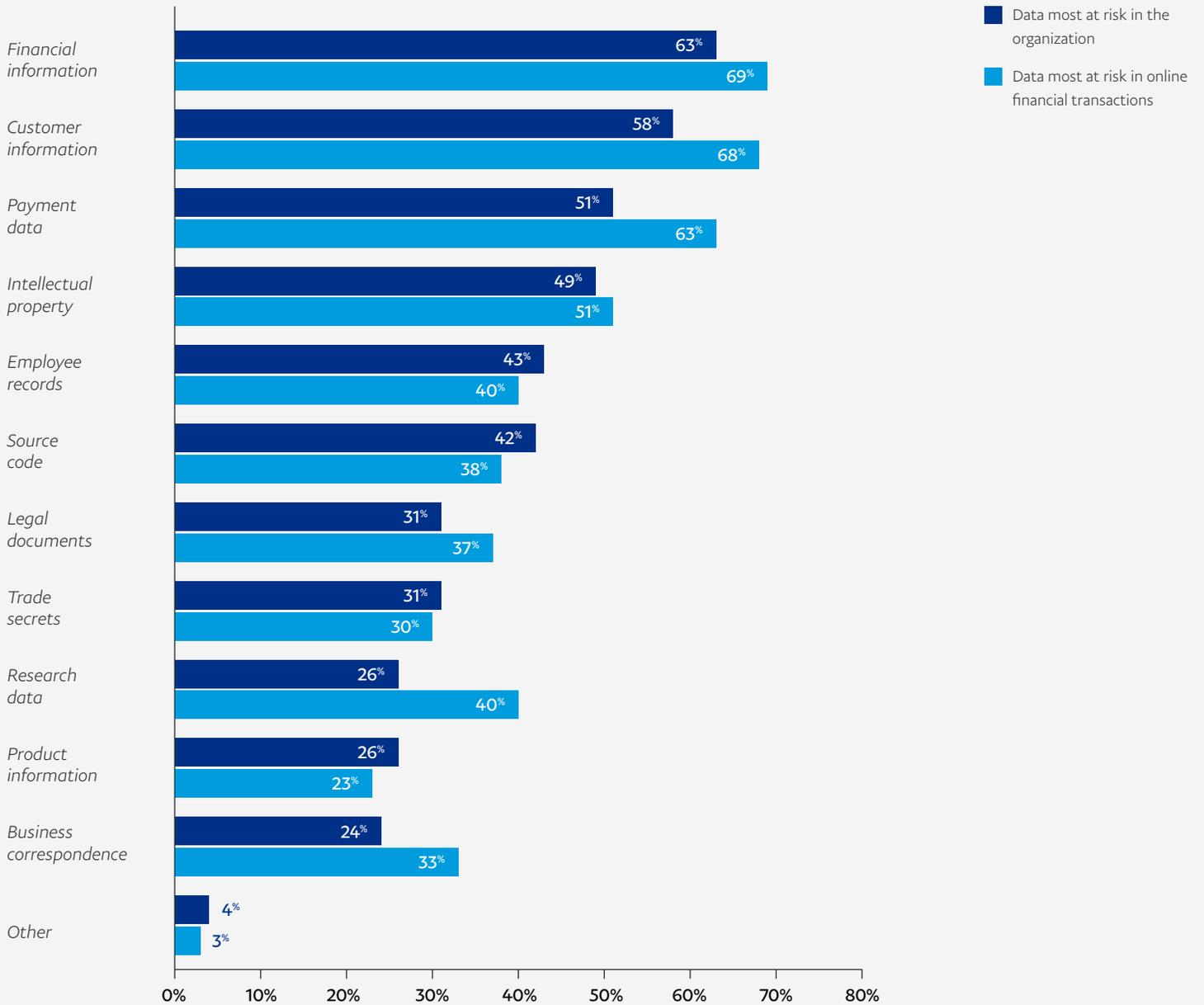
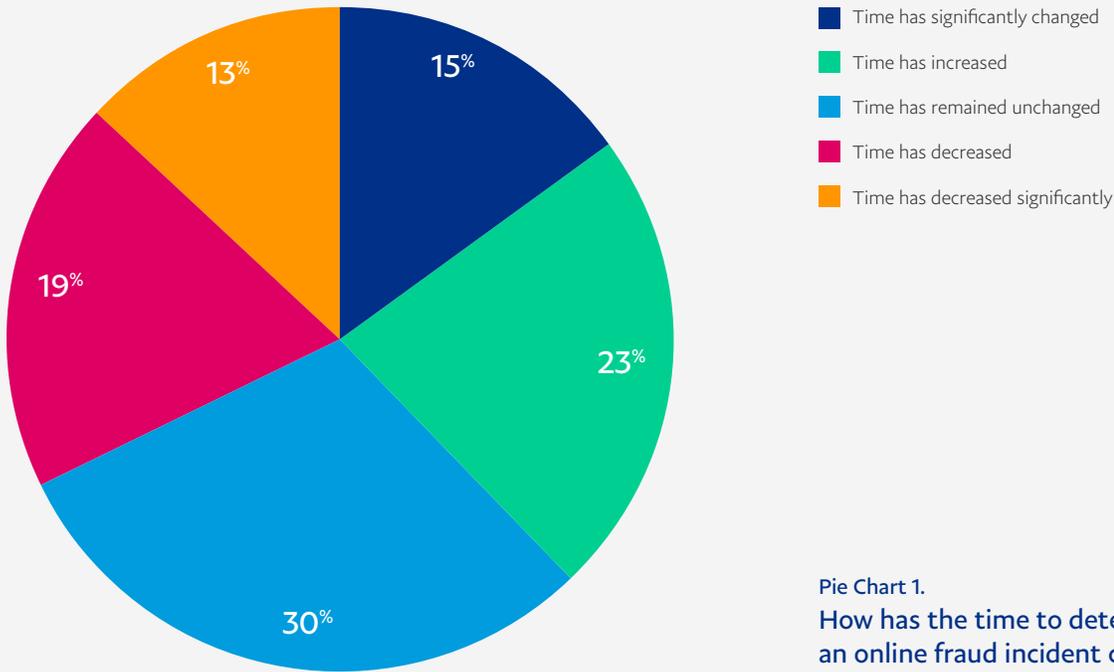


Figure 5.
Data most at risk in the organization and online
 More than one response permitted

No improvements are being made to detect, contain and respond to an online fraud incident. As shown in Pie Chart 1, 38 percent of respondents say the time it takes to detect, contain and respond to an online fraud incident has increased (23 percent) or increased significantly (15 percent) in the past 12 months. Only 32 percent of respondents say the time has decreased (19 percent) or decreased significantly (13 percent), particularly sensitive to the risk to financial information (69 percent of respondents), customer information (68 percent of respondents) and payment data (63 percent of respondents), as shown in Figure 5.



Pie Chart 1.
How has the time to detect, contain and respond to an online fraud incident changed?





Organizations' approach to securing online transactions

The top benefit of using machine learning and advanced analytics in fraud detection is better integration with threat intelligence sources. **Sixty percent say AI technologies such as machine learning, behavioral analytics, automation and orchestration are essential to detecting online fraud incidents, yet only 51 percent of respondents say their organizations use automation, machine learning and/or behavioral analytics to detect online fraud.**

According to Figure 6, the top three security benefits of using machine learning and advance analytics to detect fraud are better integration with threat intelligence sources (52 percent), increased effectiveness of security teams (50 percent) and the ability to automate routine tasks (47 percent).

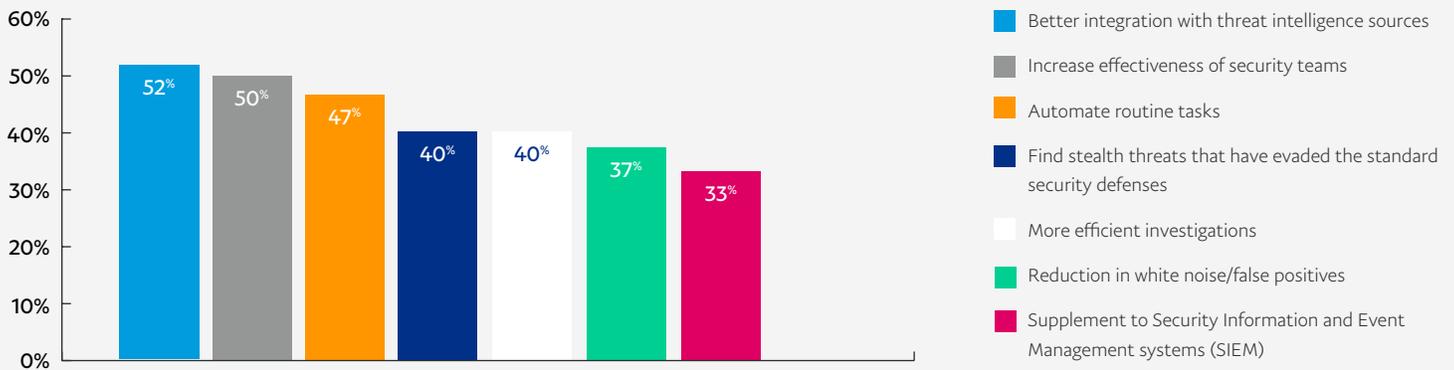


Figure 6. What are the top three key security benefits of using machine learning and advanced analytics in fraud detection?

Three responses permitted

Finding attacks before they do damage is the most important feature of automation. Respondents were asked to rate the importance of three benefits of automation on a scale of 1 = low importance to 10 = highly important. Figure 7 shows the very important responses (7+ responses). Seventy-six percent of respondents say finding attacks before they do damage and 71 percent of respondents say reducing the amount of time and effort required to investigate an alert are very important.

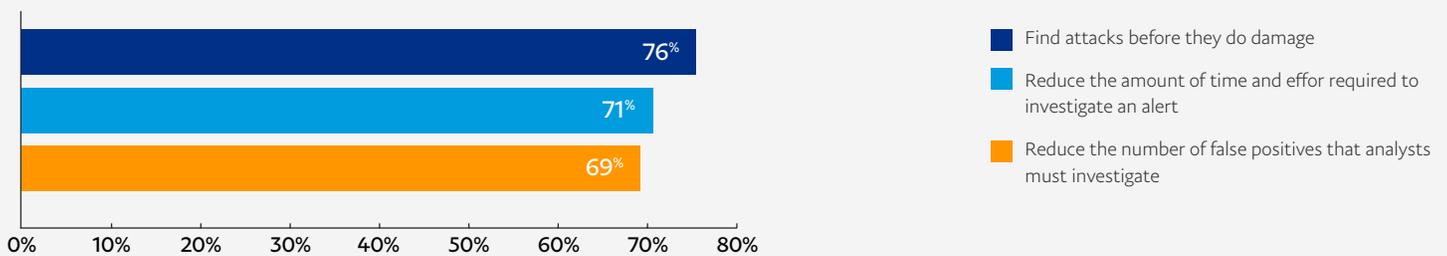


Figure 7. Automation features important to achieving a more efficient and effective online security posture

More than one response permitted

Improvements in identity authentication will improve the state of access governance. However, as shown in Figure 8, only 43 percent of respondents say their organizations implement online fraud security strategies that align with business initiatives.

The most positive step organizations can take is to improve identity authentication in order to make it more efficient to operate online (71 percent of respondents). Fifty-six percent of respondents say their online fraud security solutions and policies help balance security requirements with business enablement and 55 percent say compliance with PCI-DSS is an important objective of their organizations' anti-fraud efforts.

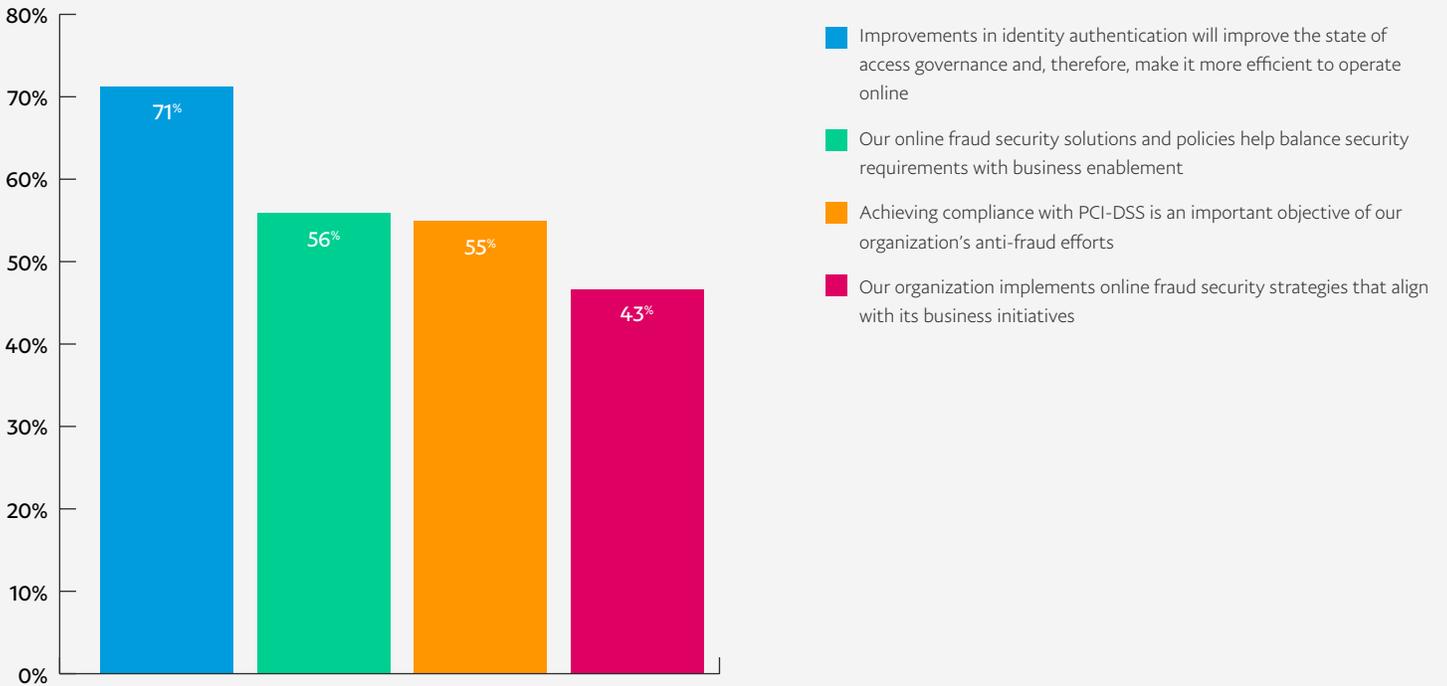


Figure 8.
Perceptions about steps to reduce online fraud
Strongly agree and Agree responses combined



To create and retain trust in online transactions, organizations have policies to ensure strict security safeguards are in place. According to Figure 9, 70 percent of respondents say their organizations have policies to ensure strict security safeguards are in place. This is followed by transparency in sensitive data used in online financial transactions.

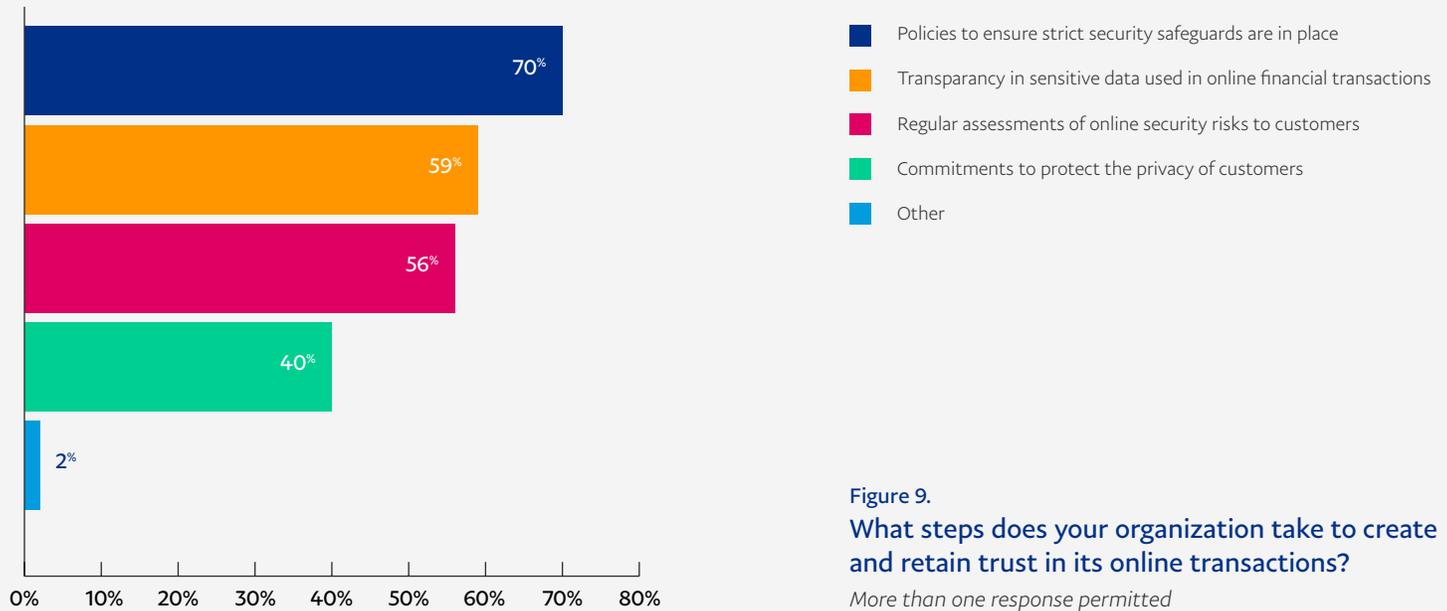


Figure 9.
What steps does your organization take to create and retain trust in its online transactions?
More than one response permitted

Collaboration between the fraud and cybersecurity teams is considered important to detecting and investigating online fraud, but not achieved. Respondents were asked to rate the level of collaboration and the importance of collaboration on a scale from 1 = no collaboration/not important to 10 = complete collaboration/very important.

Figure 10 shows the very or complete collaboration responses (7+ responses) and important and very important (7+ responses). Sixty-four percent of respondents say it is very important to have collaboration between the fraud and cybersecurity teams. However, only 29 percent of respondent say such collaboration occurs.

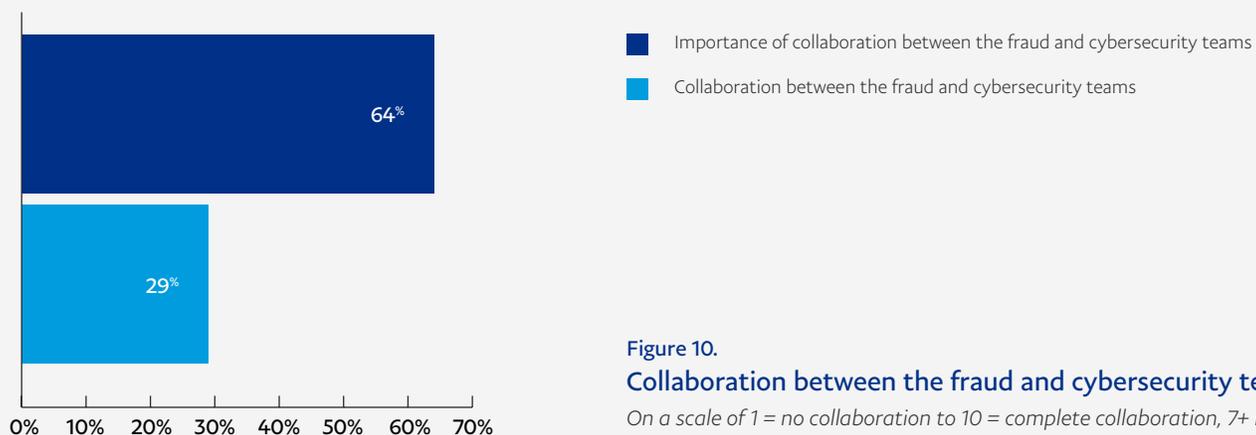


Figure 10.
Collaboration between the fraud and cybersecurity teams
On a scale of 1 = no collaboration to 10 = complete collaboration, 7+ response presented

Forty-two percent of online fraud incidents are chargeback fraud. As shown in Figure 11, the steps taken to prevent such fraud are to have clear merchant descriptors (72 percent of respondents), have clear and flexible return policies (69 percent of respondents) and respond to every dispute (64 percent of respondents) and respond to every dispute (64 percent of respondents).

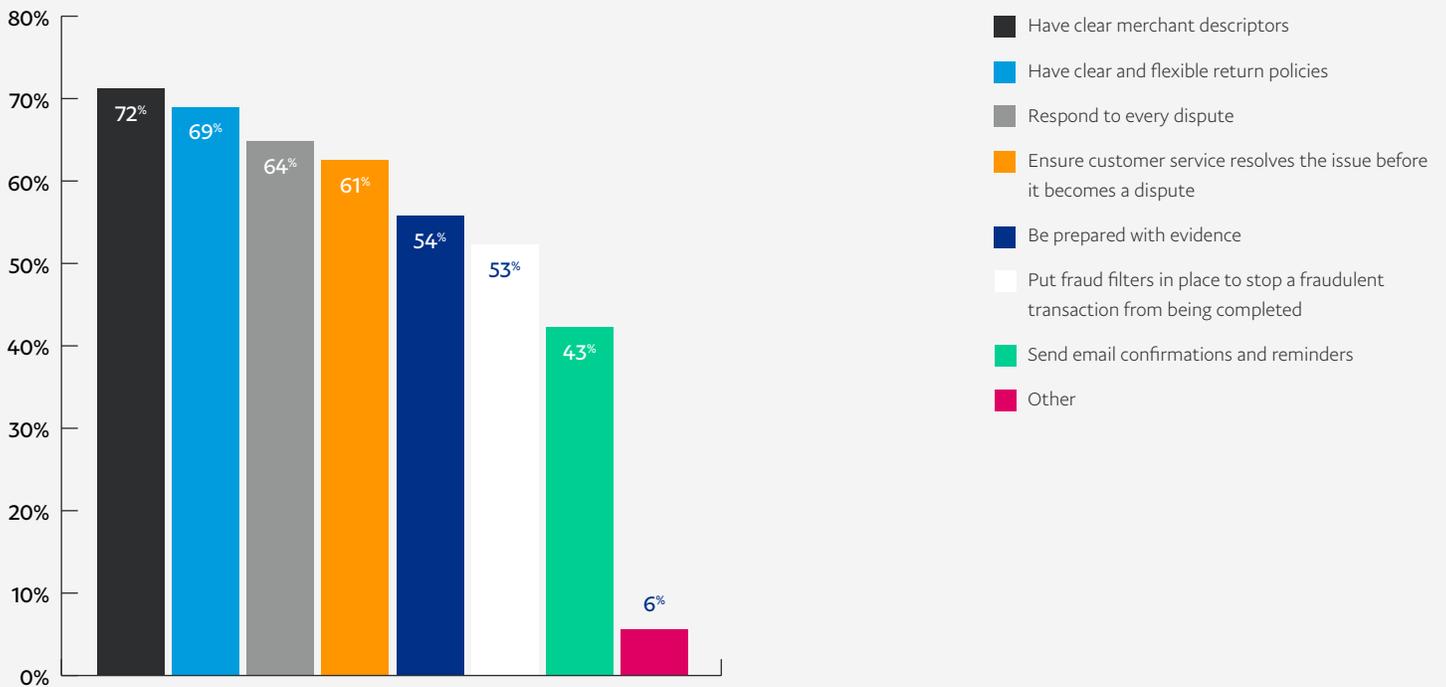


Figure 11.
What steps are taken to prevent chargeback fraud?
More than one response permitted

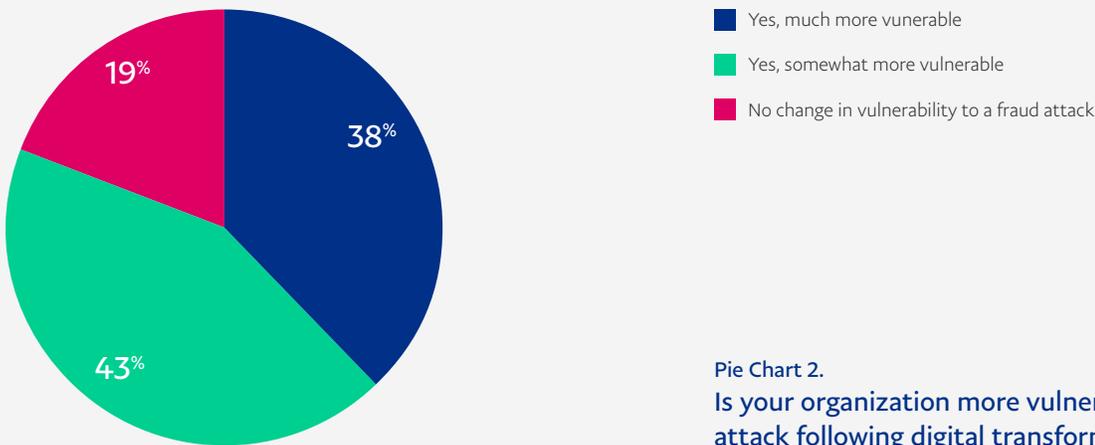




The risks of digital transformation to online security

Digital transformation is important to support business goals, but it makes online transactions more vulnerable. Eighty-three percent of respondents say digital transformation is essential (21 percent), very important (34 percent) and important (28 percent).

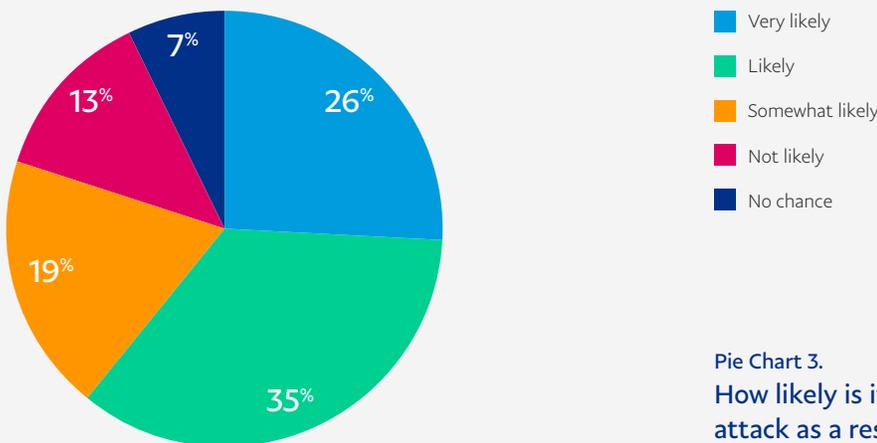
According to Pie Chart 2, 81 percent of respondents say their organizations are much more vulnerable (38 percent) or more vulnerable (43 percent) to an online fraud attack following digital transformation. When asked how concerned they are about having an online fraud incident as a result of insecure digital transformation, 79 percent of respondents say they are significantly concerned (30 percent), very concerned (31 percent) or concerned (18 percent).



- Yes, much more vulnerable
- Yes, somewhat more vulnerable
- No change in vulnerability to a fraud attack

Pie Chart 2.
Is your organization more vulnerable to an online fraud attack following digital transformation?

Most organizations believe it is likely they had an online fraud attack as a result of insecure digital transformation. As shown in Pie Chart 3, 80 percent of respondents say it was very likely (26 percent), likely (35 percent) and somewhat likely (19 percent).



- Very likely
- Likely
- Somewhat likely
- Not likely
- No chance

Pie Chart 3.
How likely is it that your organization had an online fraud attack as a result of insecure digital transformation?

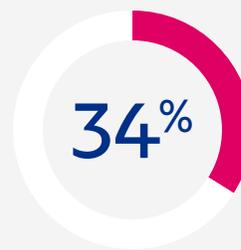


COVID-19 and online fraud

COVID-19 has made organizations more vulnerable to online fraud. Respondents were asked to rate their organizations' effectiveness in reducing online fraud prior to COVID-19 and due to COVID-19 on a scale of 1 = not effective to 10 = highly effective. As shown in Figure 12, effectiveness has declined significantly from 45 percent of respondents who rated their effectiveness as effective or very effective to 34 percent of respondents.



Reducing online fraud prior to COVID-19



Reducing online fraud due to COVID-19

Figure 12.

Effectiveness in reducing online fraud prior to COVID-19 and due to COVID-19

On a scale from 1= ineffective to 10 = very effective, 7+ response presented



As a result of the remote workforce, respondents are most concerned about the inability to secure communications on external networks outside their organizations' control, according to 55 percent of respondents. As shown in Figure 13, phishing and social engineering scams directed at teleworkers (52 percent of respondents) and the difficulty in securing the organization's network (49 percent of respondents) are also security risks.

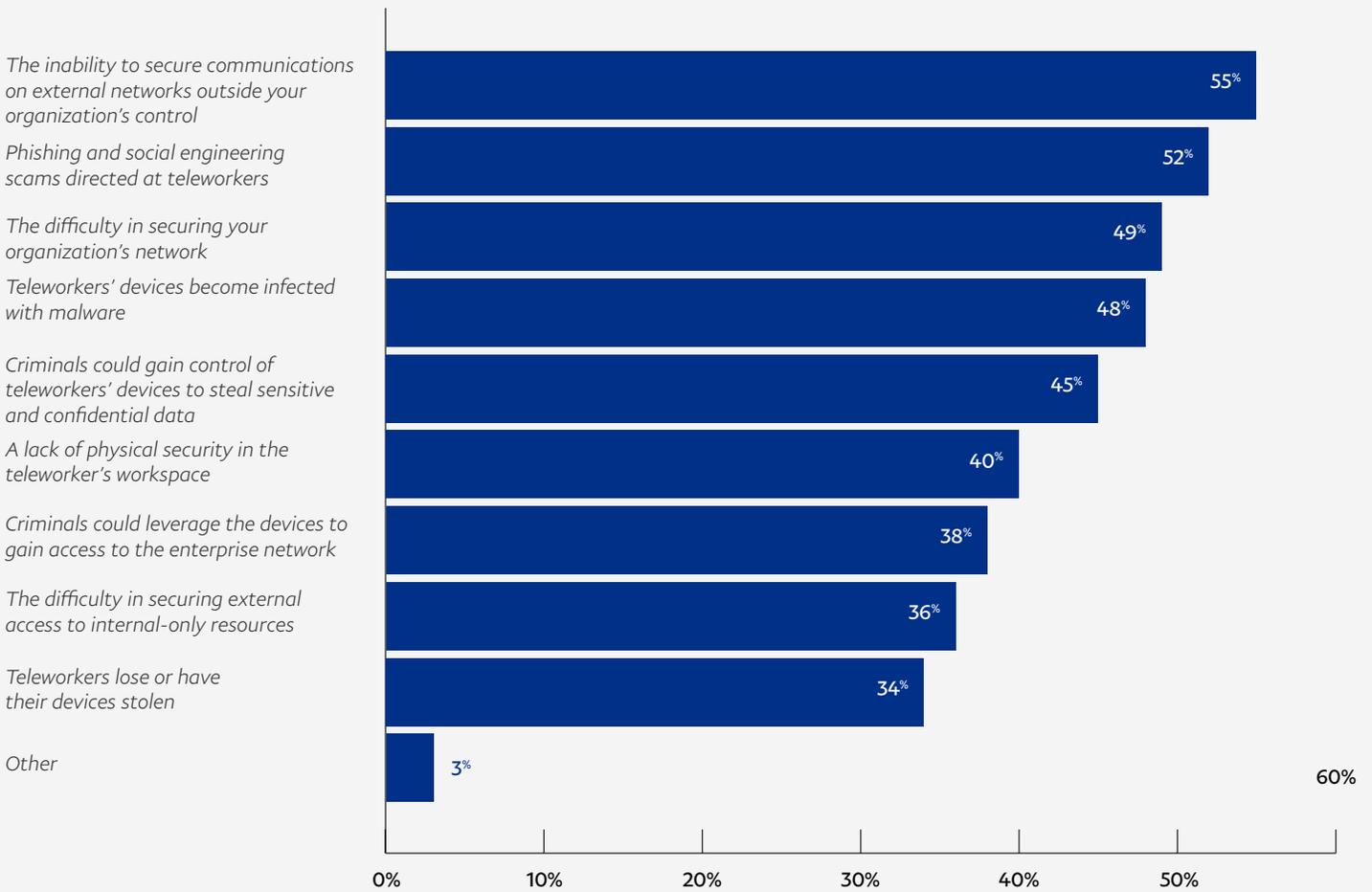


Figure 13.
The most serious risk caused by remote workers
 Four responses permitted

The risks to financial information and payment data continue in the remote worker environment. As shown in Figure 14, respondents are concerned not only about customer information (71 percent) but also financial information (70 percent) and payment data (62 percent).

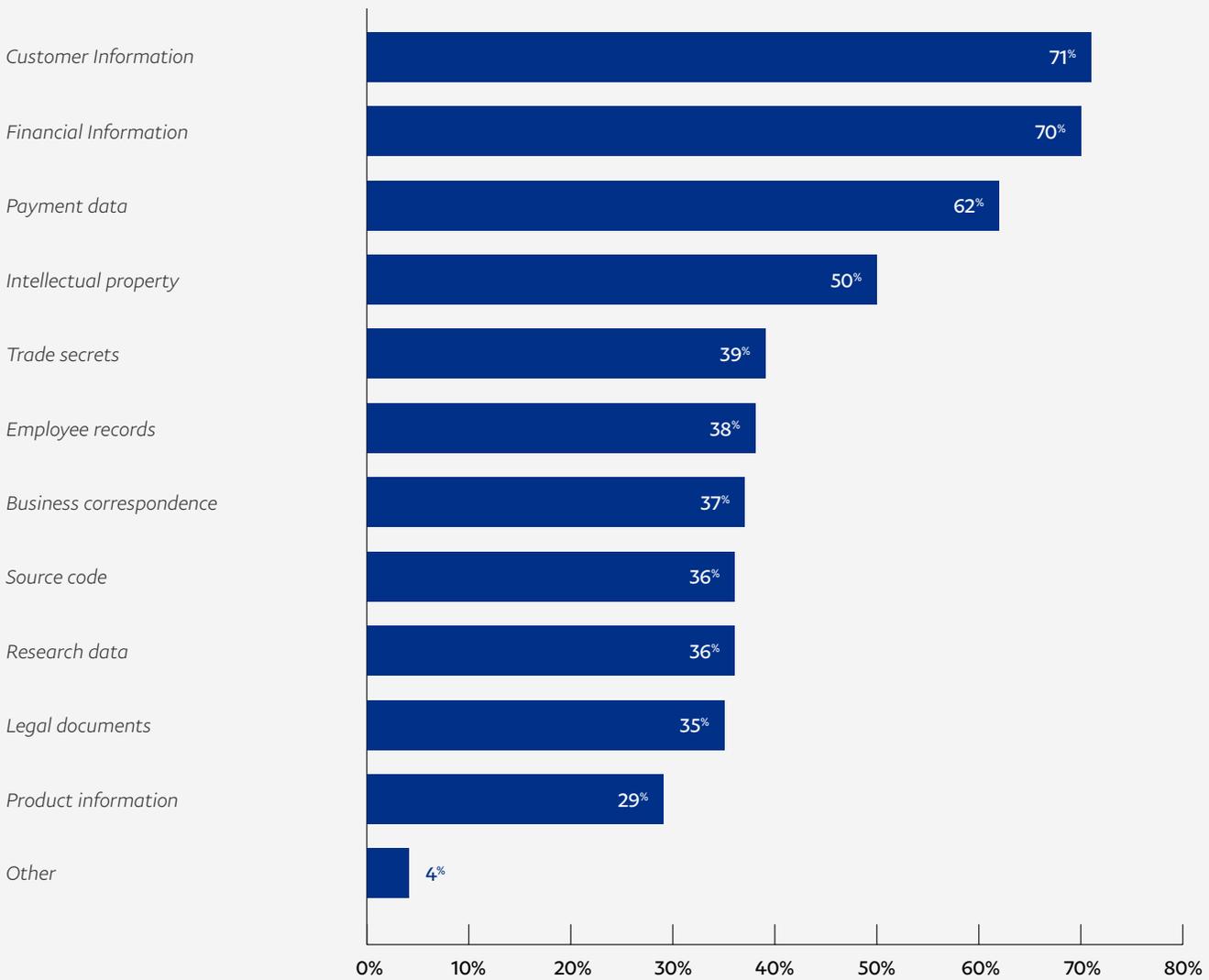


Figure 14.
Types of information most at risk in the remote worker environment
More than one response permitted

The cost of fraud and budget

Organizations represented in this research have an average of 18,492,000 online transactions and experience an average of 433 online fraud incidents annually. An average of \$4.5 million is lost per year due to online fraudulent transactions.

As shown in Figure 15, an average of 28 percent of these incidents are fraudulent and 42 percent of these incidents are chargebacks. In the context of this research, chargeback fraud is defined as the fraudulent request for a return or refund in the form of a chargeback. The customer disputes the transaction in an attempt to regain the dollar amount while retaining the product or services rendered.

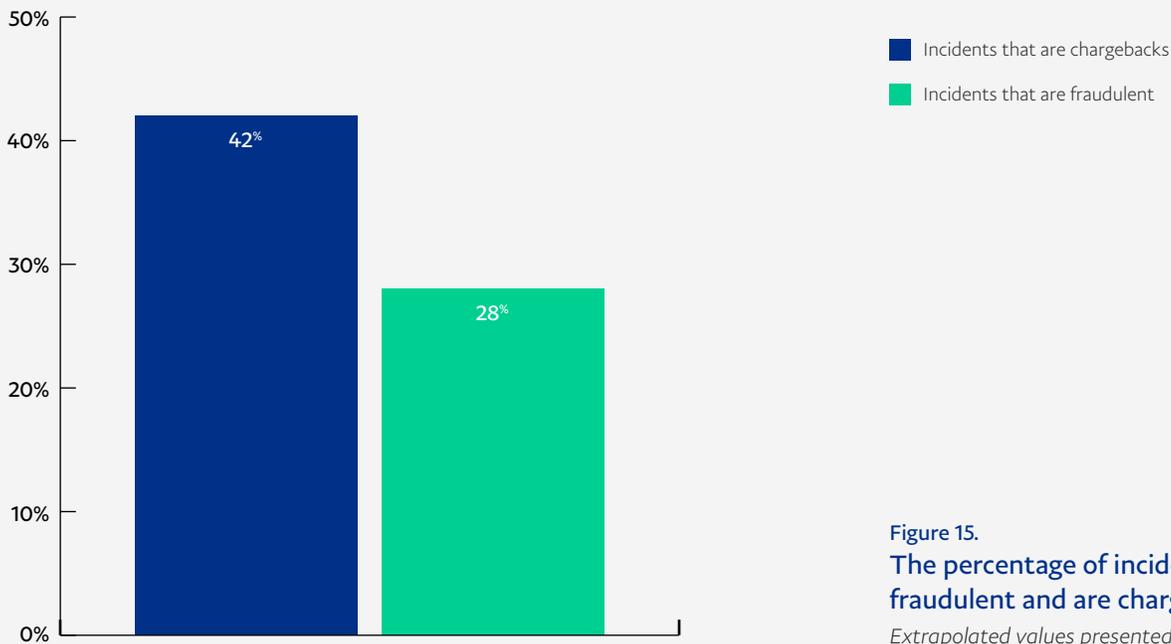


Figure 15.
The percentage of incidents fraudulent and are chargebacks
Extrapolated values presented

Table 1 presents a breakdown of the average budget assigned to IT and IT security and funding for the prevention, response and containment of an online fraud incident.

2021 IT budget	\$ 299,550,000
2021 IT budget that will go to IT security activities	\$56,914,500
IT security budget that will go to activities relating to preventing, responding to and containing an online fraud incident	\$13,659,480

Table 1.
How much organizations are spending on IT, IT security and online fraud

Table 2 provides seven cost categories of online fraud. As shown, most of the budget is allocated to operational costs, customer attrition and chargeback fraud.

Cost categories	Percentage distribution
Operational costs	21%
Legal and regulatory costs	9%
Reputation and brand damage	11%
Customer attrition	16%
Customer retention	15%
Loss of business relationships	12%
Chargeback fraud	16%
Total	100%

Table 2.
Allocation of the budget to seven cost categories of online fraud





Best practices from organizations that are highly effective in investigating online fraud

An important takeaway from this research is that there are organizations that self-report they are highly effective in investigating online fraud. We refer to these respondents as high performers who represent 23 percent of the overall sample of respondents (average performers). We do this analysis to better understand how organizations can improve their approach to investigating and reducing online fraud.

High performers are most likely to make it a priority to protect online financial transactions (60 percent of high performers vs. 48 percent of average performers) and to regularly assess the ability of its IT systems to prevent and contain online financial fraud (58 percent of high performers vs. 44 percent of average performers). **High performers make it a priority to use fraud solutions that effectively balance fraud prevention with business enablement growth, according to Figure 16.**

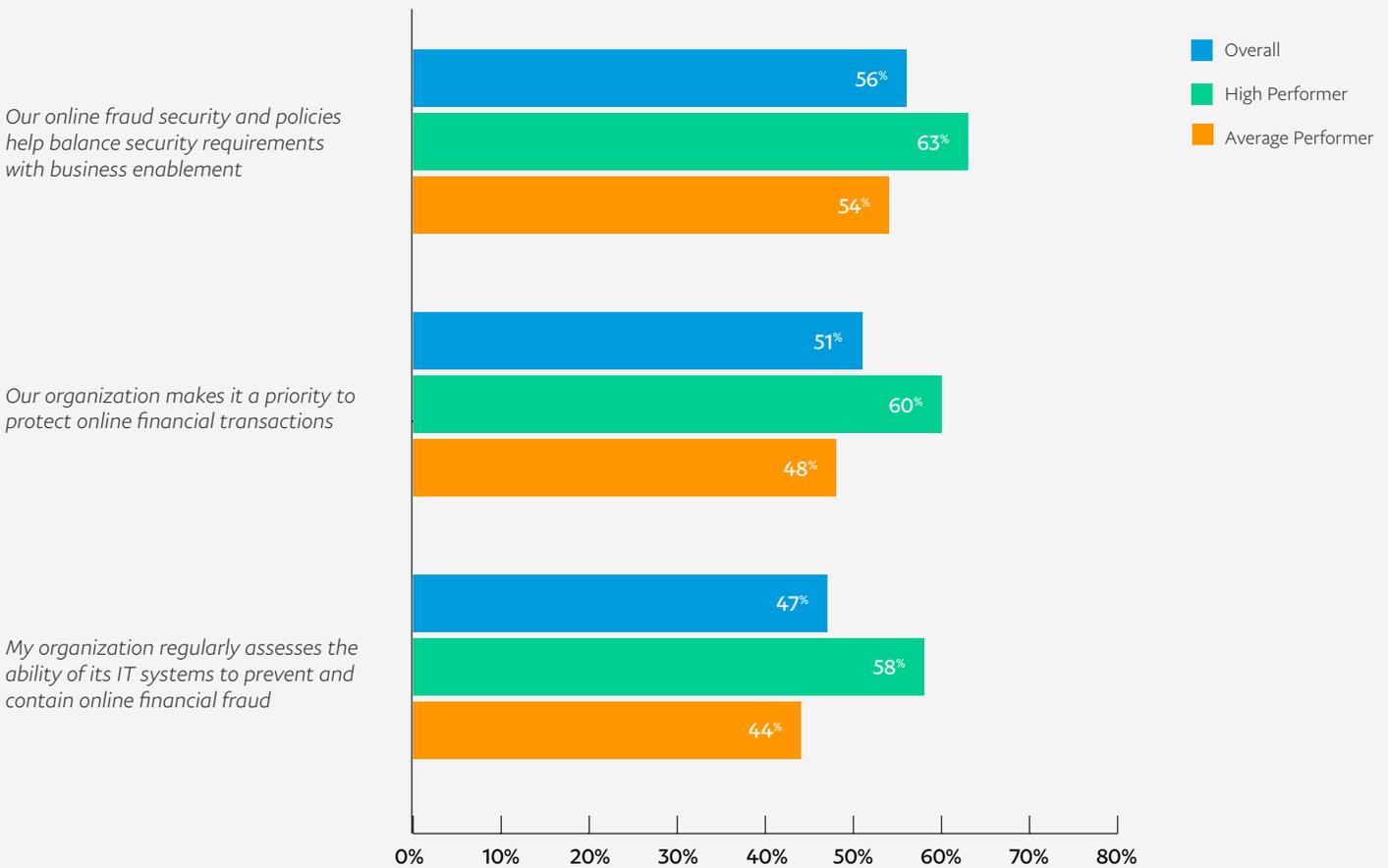


Figure 16.
Perceptions about online fraud
 Strongly agree and Agree responses combined

As shown in Figure 17, high performers are far more effective in investigating online fraud (55 percent of high performers vs. 42 percent of average performers), preventing chargeback fraud (58 percent of high performers vs. 33 percent of average performers) and achieving compliance with IT security and privacy regulations (53 percent of high performers vs. 30 percent of average performers).

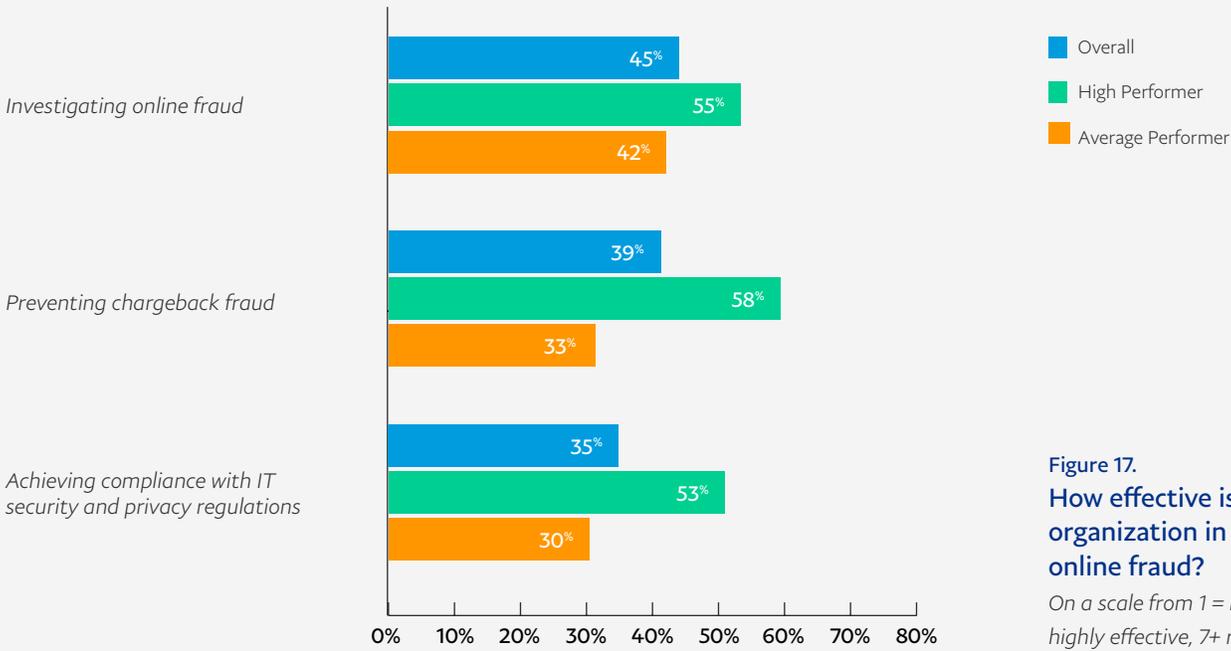


Figure 17.
How effective is your organization in investigating online fraud?
 On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented

More high performers have a team dedicated to detecting and containing online fraud, as shown in Figure 18.

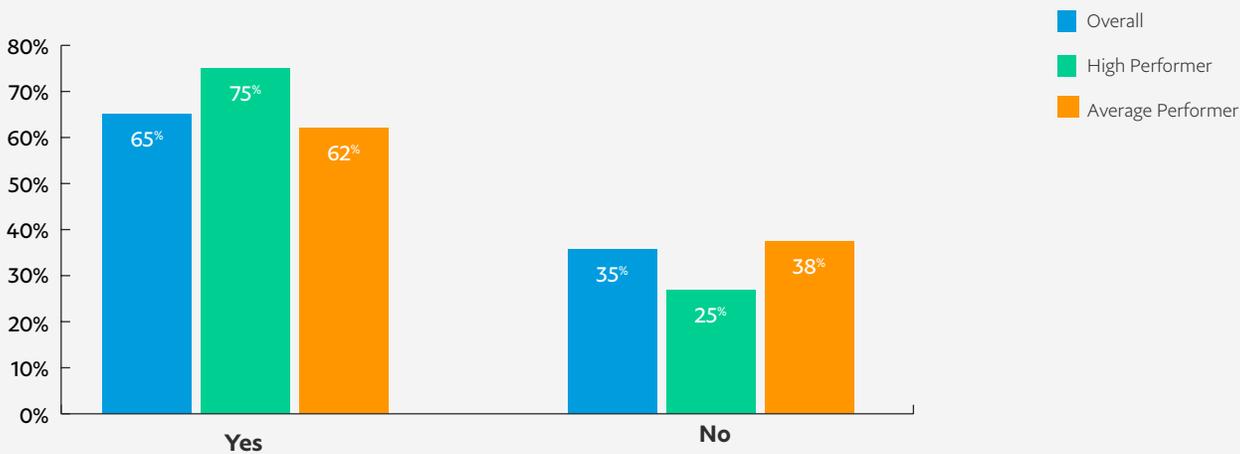


Figure 18.
Does your organization have a team dedicated to detecting, responding to and containing online fraud?

As shown in Figure 19, 63 percent of **high performing organizations use automation, machine learning and behavior analysis to detect online fraud compared to only 47 percent of average performers.**

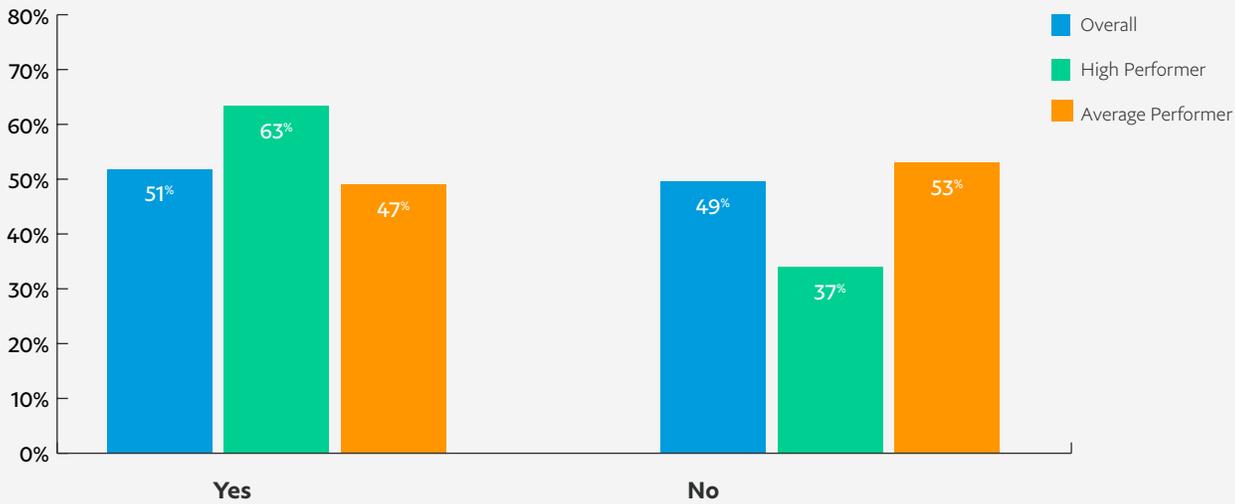


Figure 19. Does your organization use automation, machine learning and behavior analysis to detect online fraud?

Further, 71 percent of respondents in high performing organizations say AI technologies are essential to detecting online fraud incidents as compared to 57 percent of average performers, as shown in Figure 20.

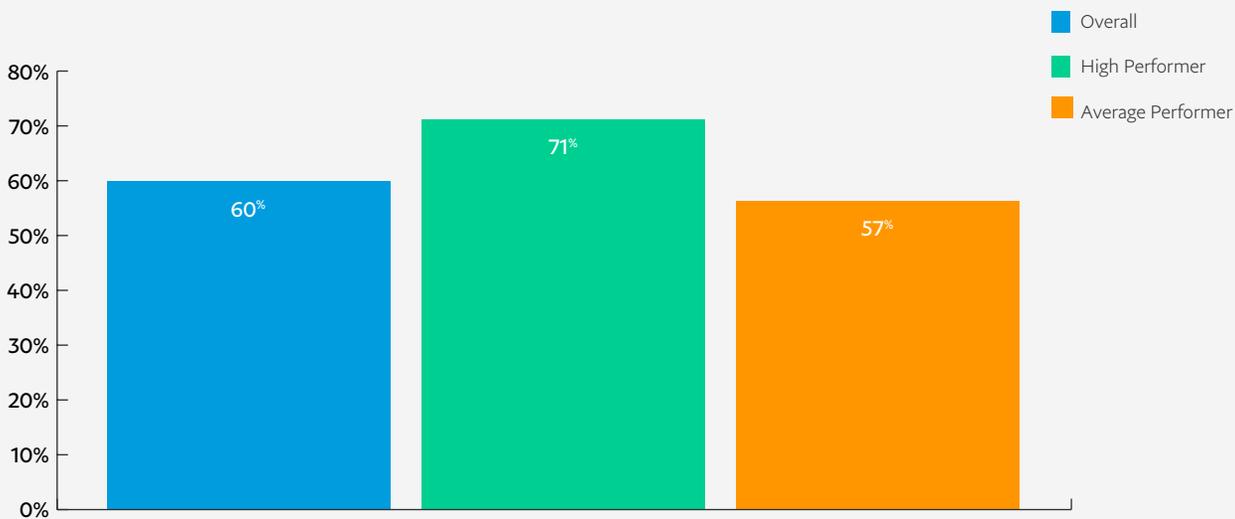


Figure 20. AI technologies are essential to detecting online fraud incidents
Strongly agree and Agree responses combined

As shown in Figure 21, both high performers and average performers agree the top three benefits are automation of routine tasks, better integration with threat intelligence sources and the ability to find stealthy threats that evaded the standard security defenses.

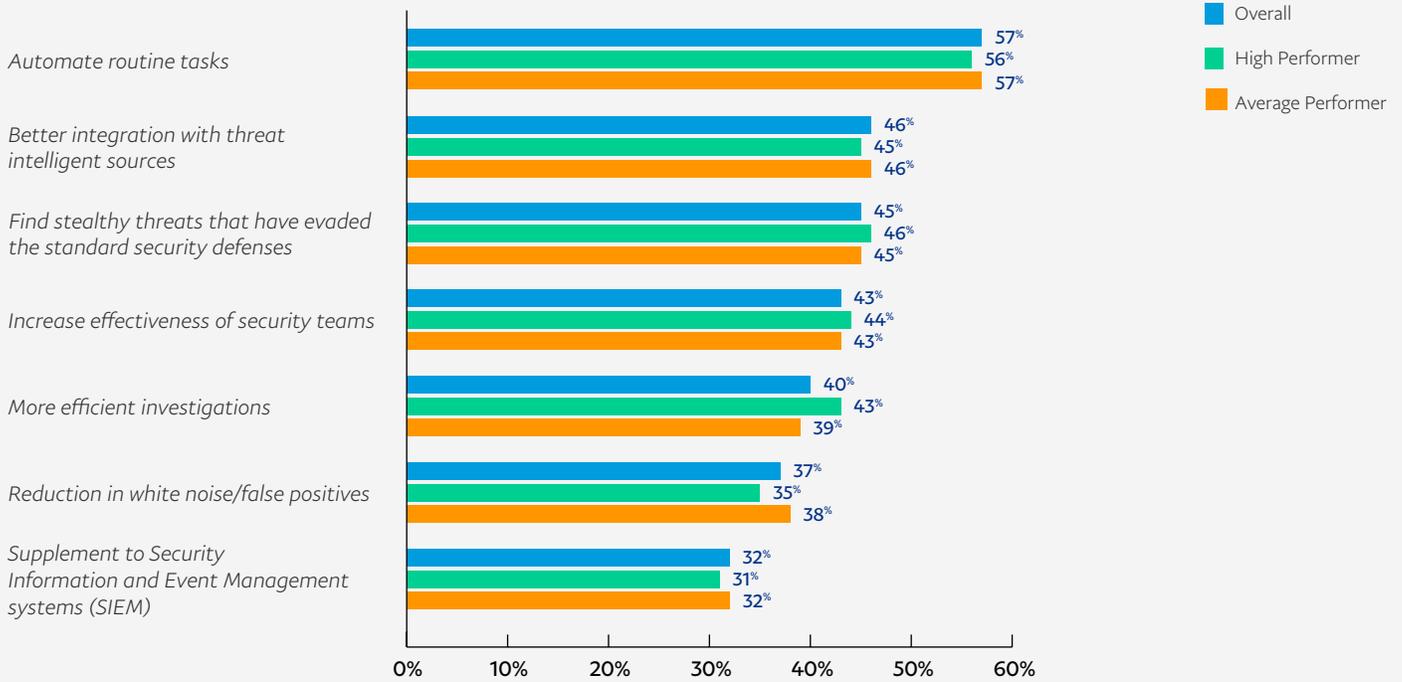
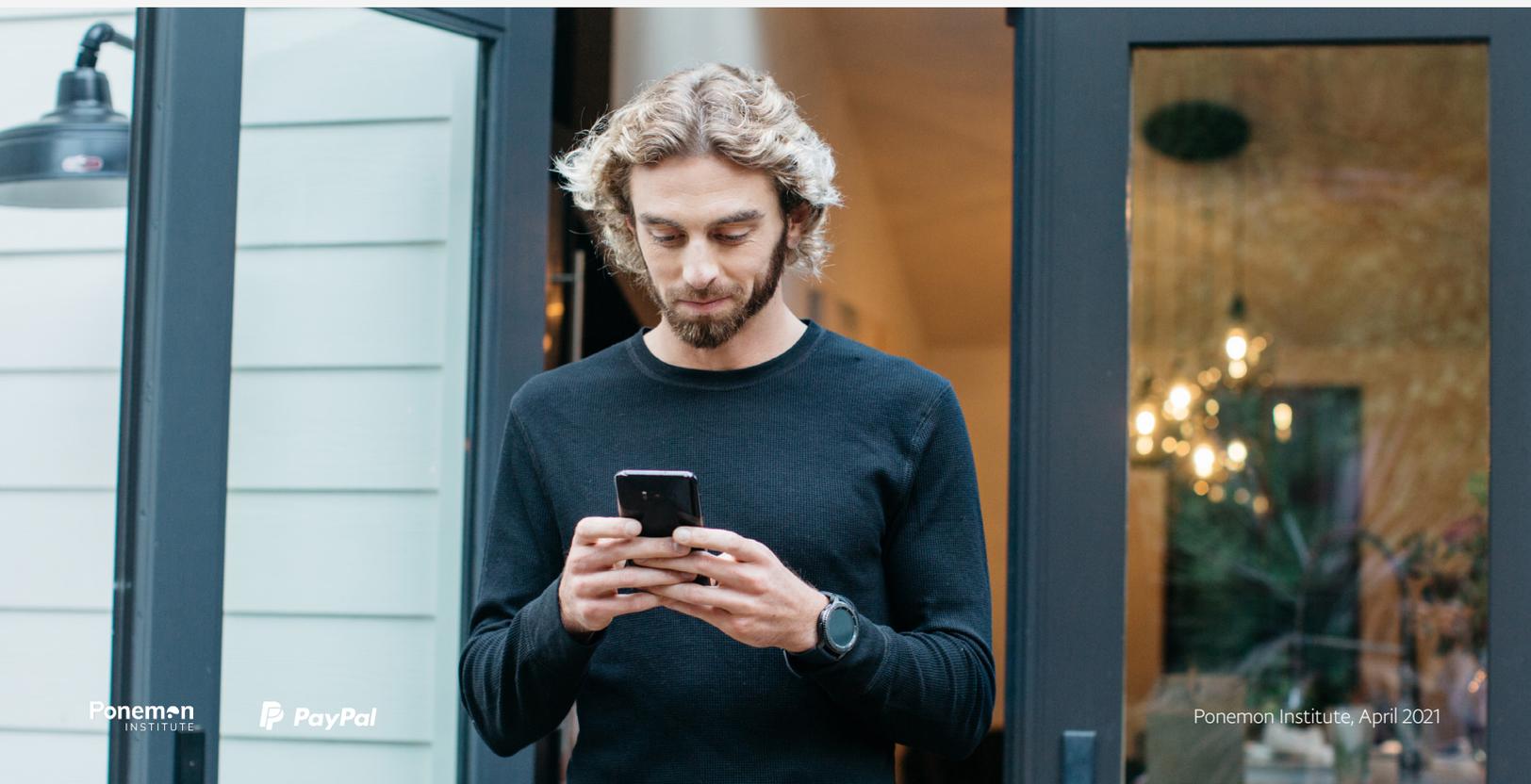


Figure 21. What are the top three key security benefits of using ML and advanced analytics in fraud detection?

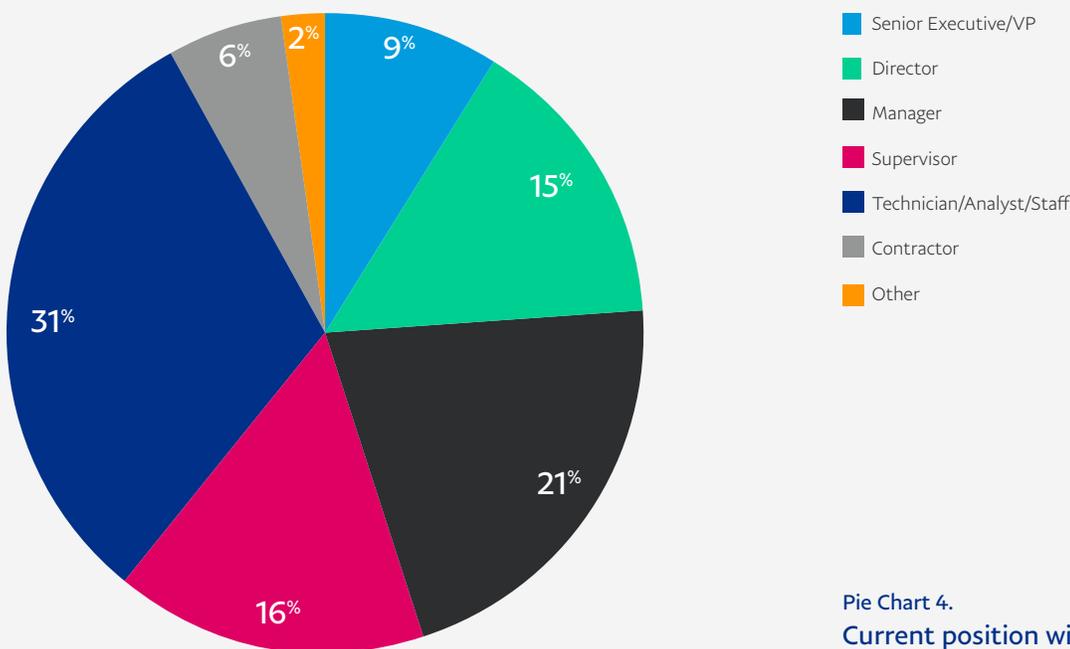


Methods

A sampling frame of 16,434 individuals who are familiar with their organizations' efforts to mitigate fraud and involved in fraud investigation and mitigation and/or cybersecurity activities were selected as participants to this survey. Table 3 shows 689 total returns. Screening and reliability checks required the removal of 57 surveys. Our final sample consisted of 632 surveys or a 3.8 percent response.

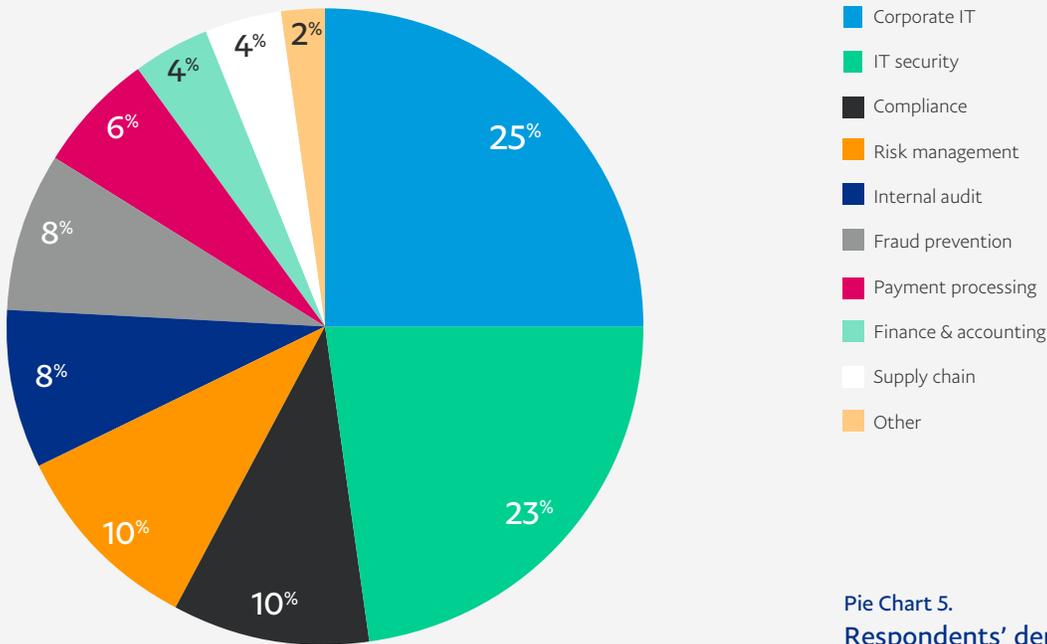
Table 3. Sample response	Freq	Pct%
Sampling frame	16,434	100.0%
Total returns	689	4.2%
Rejected or screened surveys	57	0.3%
Final sample	632	3.8%

Pie Chart 4 reports the respondent's organizational level within participating organizations. By design, more than half (61 percent) of respondents are at or above the supervisory levels. The largest category at 31 percent of respondents is technician/analyst/staff.



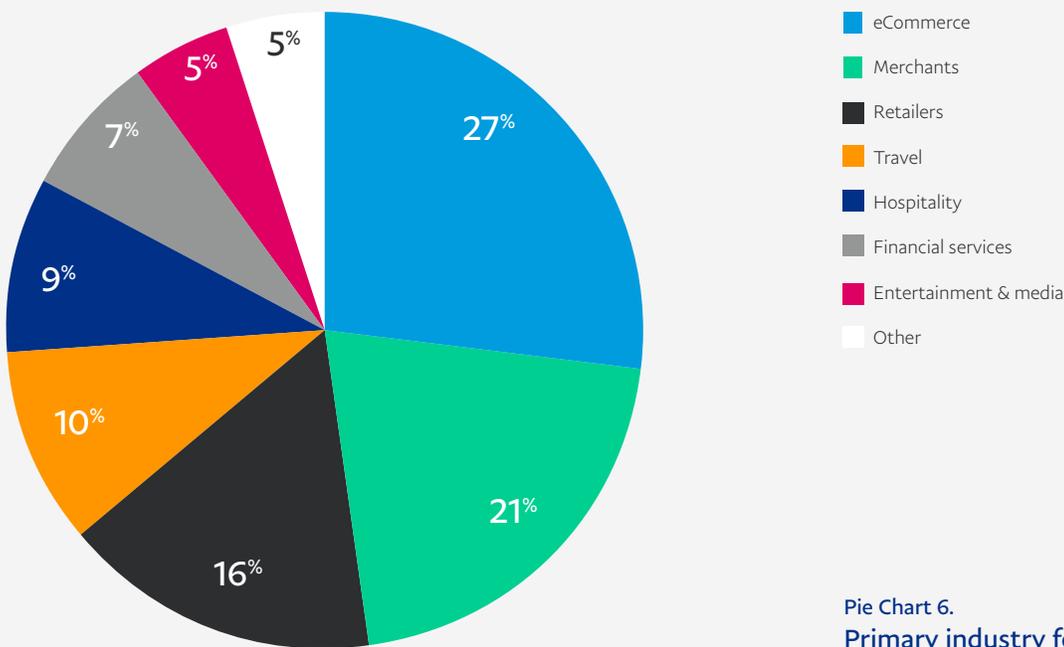
Pie Chart 4.
Current position within the organization

According to Pie Chart 5, 25 percent of respondents are located within corporate IT. This is followed by IT security (23 percent of respondents), compliance (10 percent of respondents), and risk management (10 percent of respondents).



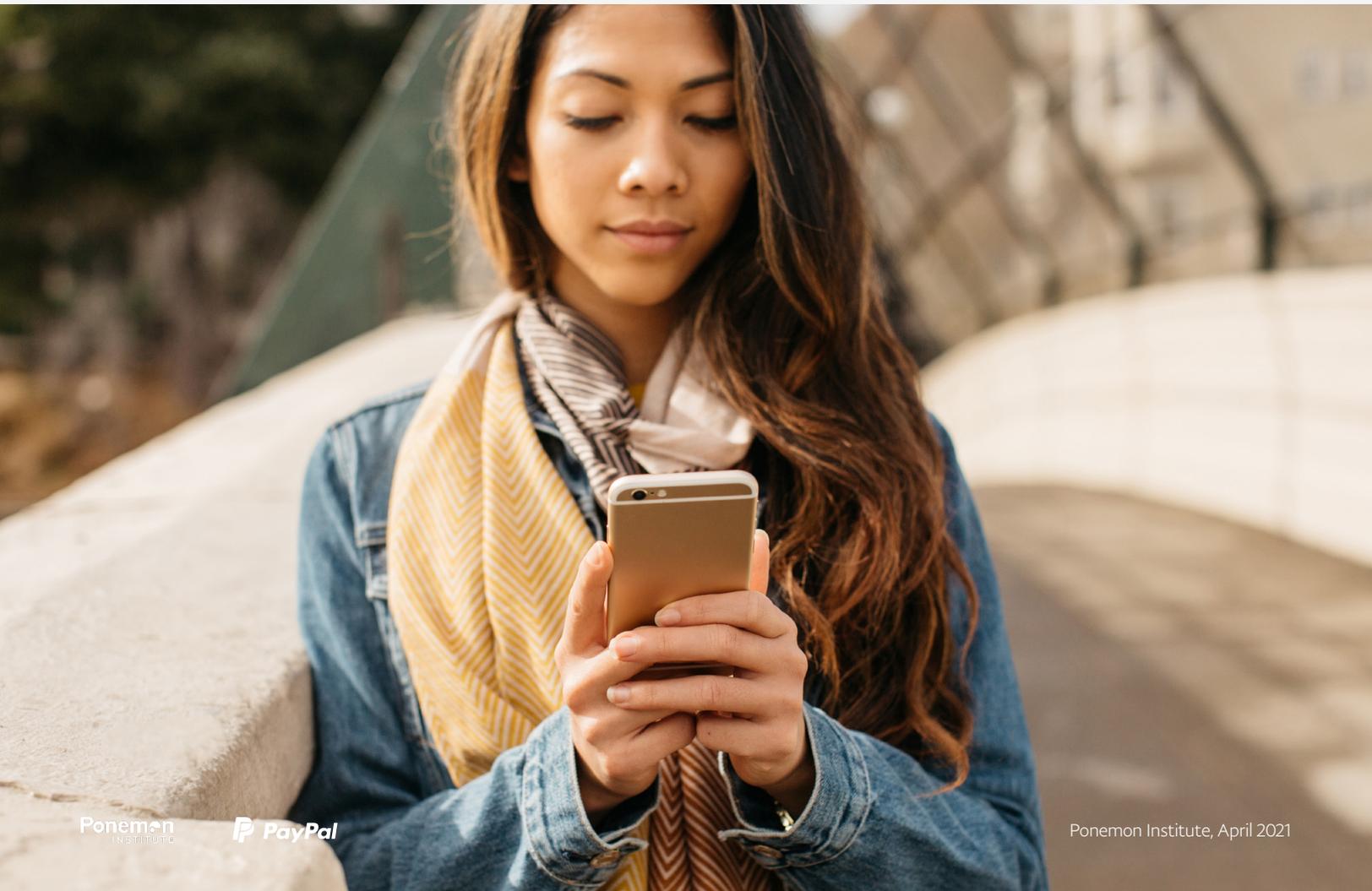
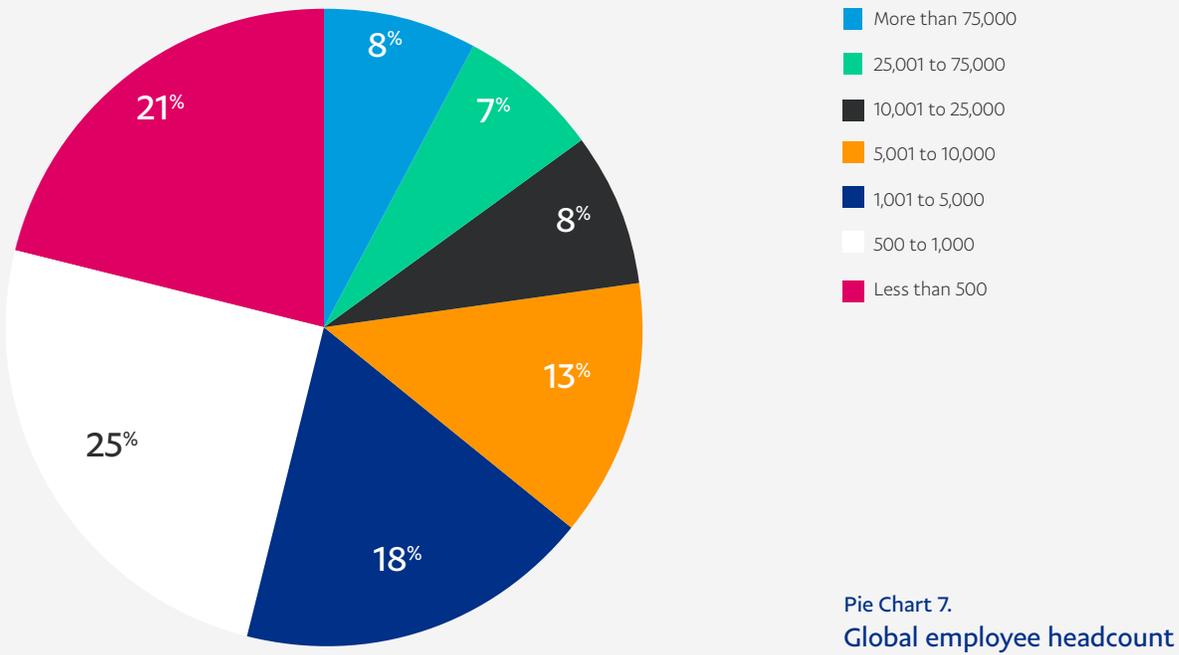
Pie Chart 5.
Respondents' department or team

Pie Chart 6 reports the industry classification of respondents' organizations. This chart identifies eCommerce (27 percent) as the largest industry focus. This is followed by merchants (21 percent of respondents), retailers (16 percent of respondents), and travel (10 percent of respondents).



Pie Chart 6.
Primary industry focus

As shown in Pie Chart 7, 54 percent of respondents are from organizations with a global headcount of more than 1,000 employees.



Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias

The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias

The accuracy is based on contact information and the degree to which the list is representative of individuals who are familiar with their organizations' efforts to mitigate fraud and involved in fraud investigation and mitigation and/or cybersecurity activities. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-reported results

The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Ponemon Institutes **Advancing Responsible Information Management**

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.