The true cost of online fraud

A 2022 global study

Conducted by the Ponemon Institute and sponsored by PayPal

PayPal | Ponemon INSTITUTE

Contents

Introduction

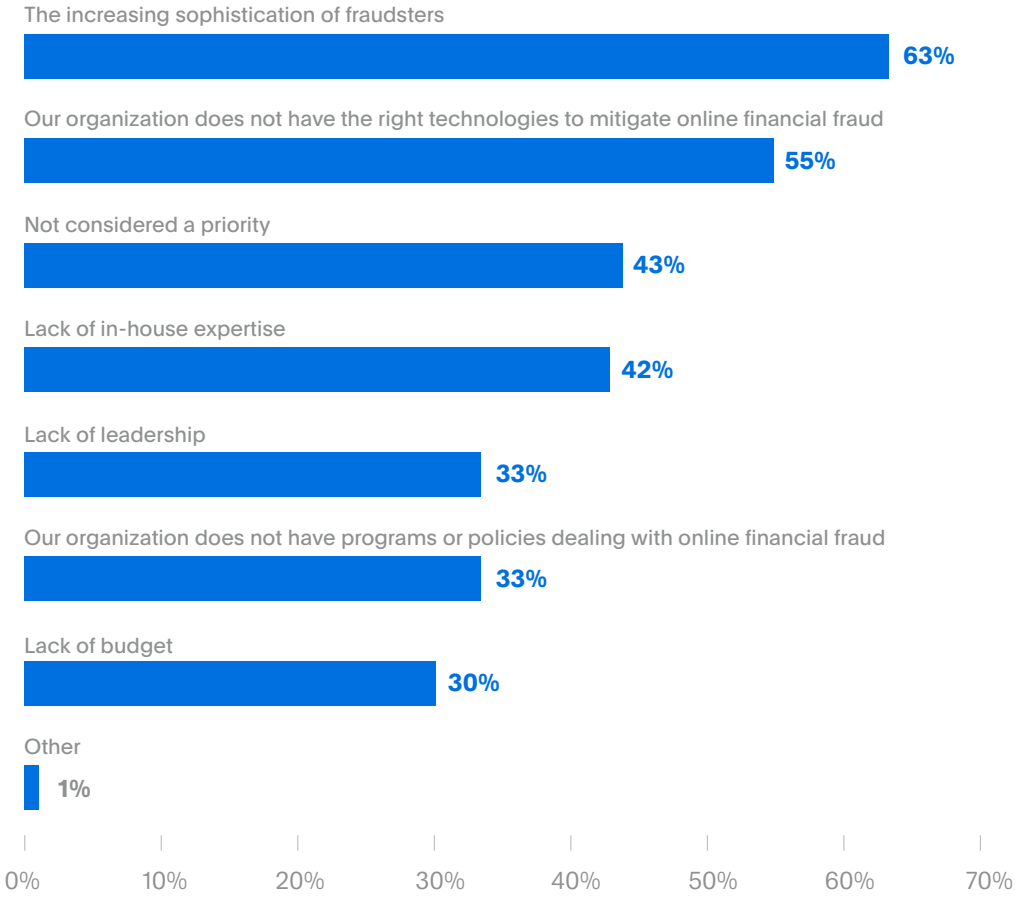
Ensuring secure online transactions is critical to maintaining customers' confidence and trust when purchasing products and services. However, as shown in this research, organizations struggle with achieving the right balance between preventing failed transactions and having a secure payment process.

Sponsored by PayPal, Ponemon Institute surveyed 3,739 individuals in the United States (442), Canada (468), Australia (475), United Kingdom (471), France (462), Germany (453), and European Cluster (968) who are involved at some level in deciding which tools/solutions their organizations use for accepting payments and how it completes credit card and debit card transactions from customers or risk solutions.

According to the research, only slightly more than half (52%) of respondents say their organizations are highly effective at reducing online fraud and less than half (47%) of respondents say they are highly effective at investigating online fraud. Accordingly, organizations represented in this research lose an average of $3.7 million per year due to fraudulent online transactions.

As shown in Figure 1, the primary challenges to mitigating online financial fraud are the increasing sophistication of fraudsters (63% of respondents), not having the right technologies to mitigate online financial fraud (55% of respondents) and not considering it a priority (43% of respondents).

Figure 1. What are the primary challenges to mitigating online financial fraud? *Three responses permitted*



The following findings provide guidance on reducing online fraud risks.

The types of data most at risk are those used in online transactions. 62% of respondents say customer information and 58% of respondents say financial information are most at risk. This is followed by 54% of respondents who say payment data is most at risk. Of far less concern to organizations are legal documents, research data, business correspondence and product information.

62% of respondents say customer information and 58% of respondents say financial information are most at risk.

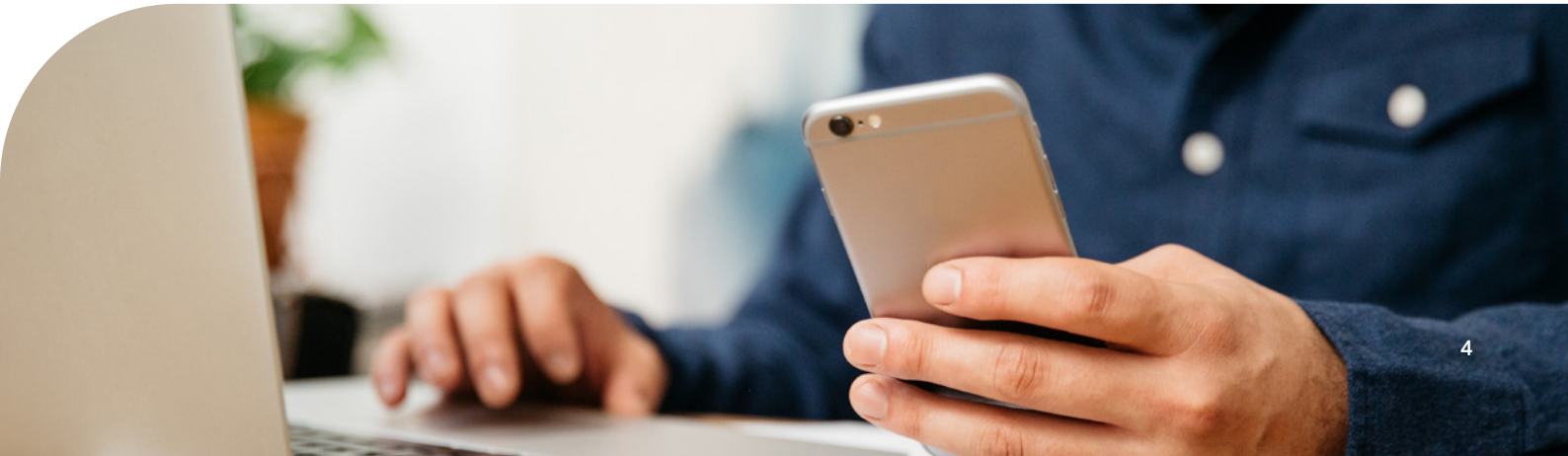
A lack of in-house expertise and fraud assessments hinder the ability to fight online fraud. Only 42% of respondents say their organizations have the necessary in-house expertise to identify and prevent e-commerce fraud and only 44% of respondents say their organizations regularly assess the ability of their payments infrastructure to prevent and contain online financial fraud.

To minimize revenue losses, organizations should prioritize the protection of customer data. The most significant payment risk, according to 56% of respondents, is the theft of customer data due to the increasing sophistication of fraudsters. This is followed by false declines (53% of respondents), which is defined as a legitimate transaction blocked by fraud prevention systems. This occurs when something about the transaction gets inaccurately flagged as fraudulent.

To avoid customer turnover, organizations' online payment processes need to be considered secure and trustworthy. The primary step taken by organizations to create and retain customers' trust in online transactions is to have policies to ensure strict security safeguards are in place (69% of respondents). This is followed by transparency in sensitive data used in online financial transactions (59% of respondents) and regular assessments of the online security risks to customers (53% of respondents).

Organizations face the challenge of being able to quickly respond to online fraud incidents. On average, organizations represented in this research have 8.78 million online transactions annually and of these an average of 29% or 2.5 million are compromised annually. Organizations are spending an average of 14 days to respond to one online fraud incident. According to the research, only 34% of respondents say the time to detect, contain and respond to an online fraud incident has decreased (19% of respondents) or decreased significantly (15% of respondents). As a result, organizations are at great risk for the theft of customer and financial information.

On average, organizations represented have 8.78 million online transactions annually and of these an average of **2.5 million are compromised.**



Digital transformation creates online fraud risks. 53% of respondents say they are familiar with their organizations' strategy for achieving digital transformation. 80%of these respondents say their organizations are much more vulnerable (42%) or vulnerable (39%) to an online fraud attack due to digital transformation.

Further, 59% of respondents say their organizations are significantly concerned about having an online fraud incident caused by insecure digital transformation and 56% of respondents say it is very likely an online fraud attack will occur due to insecure digital transformation. Because of digital transformation risks, organizations should consider leveraging advanced technologies, such as automation and AI, to detect online fraud.

80% of respondents say their organizations are much more vulnerable or vulnerable to an online fraud transformation.

Most organizations are using a team fully dedicated to detecting, responding, and containing online fraud and preventing chargebacks. 64% of respondents say their organizations have a team fully dedicated to detecting, responding, and containing online fraud. An average of 7 staff are on the fraud team. Despite the use of fraud teams, only slightly more than half (52%) of respondents say their organizations are highly effective at reducing online fraud. Less than half (47%) say their organizations are highly effective in investigating fraud.

Four members of the fraud team are fully dedicated to chargebacks. An average of 679 chargeback frauds are experienced each month and on average 31 hours are spent to investigate and respond to chargeback fraud each month. According to the research, the top two steps taken to prevent chargeback fraud are clear merchant descriptors (65% of respondents) followed by clear and flexible return policies (64% of respondents). Only slightly more than half (51%) of respondents say their organizations are prepared with evidence.

The lack of collaboration between the fraud function and cybersecurity teams can be a barrier to minimizing online fraud. While 60% of respondents say collaboration between the fraud and cybersecurity teams is very important, only 25% of respondents say complete collaboration has been achieved. One possible reason for the difficulty in achieving collaboration is that important decisions are divided between the fraud function and IT security instead of being cohesive. Specifically, the fraud function directs the online fraud prevention strategies while IT security allocates the budget for technologies used to reduce online fraud.

Fraud prevention, legal and the chief risk officer are most involved in making fraud prevention decisions. Almost half (49%) of respondents who are most involved in determining how best to secure online transactions without losing revenues are in fraud prevention, legal and the risk functions. In contrast, only 25% of IT and IT security are most involved in these decisions.

Online fraud strategies are not supportive of business initiatives and enablement. Less than half (46%) of respondents say their fraud security solutions and policies help balance security requirements with business enablement and only 44% of respondents say online fraud security strategies are aligned with business initiatives.

AI and machine learning are considered essential to the detection of online fraud. The most frequently used technologies are AI (61% of respondents), machine learning (58% of respondents and orchestration (50% of respondents). 53% of respondents who use these technologies say they are very essential and the top security benefits are better integration with threat intelligence sources and to find stealthy threats that have evaded the standard security defenses.

The primary benefit of automation is greater efficiencies in the investigation of online fraud. As discussed, 67% of respondents say their organizations use an automation layer to optimize fraud protection and authorization rates. Most respondents are getting value out of automation. The number one benefit is the reduction in the number of false positives that analysts must investigate (64% of respondents) followed by reduction in the time and effort required to investigate an alert (62% of respondents). Automation is also considered helpful in finding attacks before they do damage (59% of respondents).

Compliance is not an important part of the organizations' online fraud prevention strategy. Only 46% of respondents say achieving compliance with regulations is considered an important objective of anti-fraud efforts and only 44% of respondents say compliance with regulations is the minimum standard for achieving a strong security posture.

While most organizations are effective in preventing lost sales at the checkout, they struggle to balance strong fraud protection with preferred payment methods. 59% of respondents say their organizations are very or highly effective in keeping customer data current and preventing lost sales at the checkout. 57% of respondents say their organizations are very or highly effective in having both strong fraud protection and positive authorization rates.

> Organizations have lost an average of between **$1.5 million to more than $10 million each year.**

Customer sales are frequently lost due to transactions being declined. 49% of respondents say their organizations calculate lost revenue due to online fraud. According to these respondents, organizations have lost an average of between $1.5 million to more than $10 million each year. While less than half (47%) of respondents say their customers have frequently abandoned a shopping cart when their preferred payment is unavailable. 56% of respondents say transactions are being frequently declined.

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.

- Challenges to reducing fraud risk in online transactions
- Securing online transactions with automation and other technologies
- The use of fraud teams to prevent and detect online fraud
- Organizations' online compliance and governance practices
- Organizations' approach to reducing chargeback fraud
- The impact of online fraud on revenues, cost, and budget

Challenges to reducing fraud risk in online transactions

The types of data most at risk in organizations are those used in online transactions. As shown in Figure 2, 62% of respondents say customer information and 58% of respondents say financial information are most at risk. This is followed by 54% of respondents who say payment data is most at risk. Of far less concern to organizations are legal documents, research data, business correspondence and product information.

Figure 2. What types of data are most at risk in your organization? *More than one response permitted*

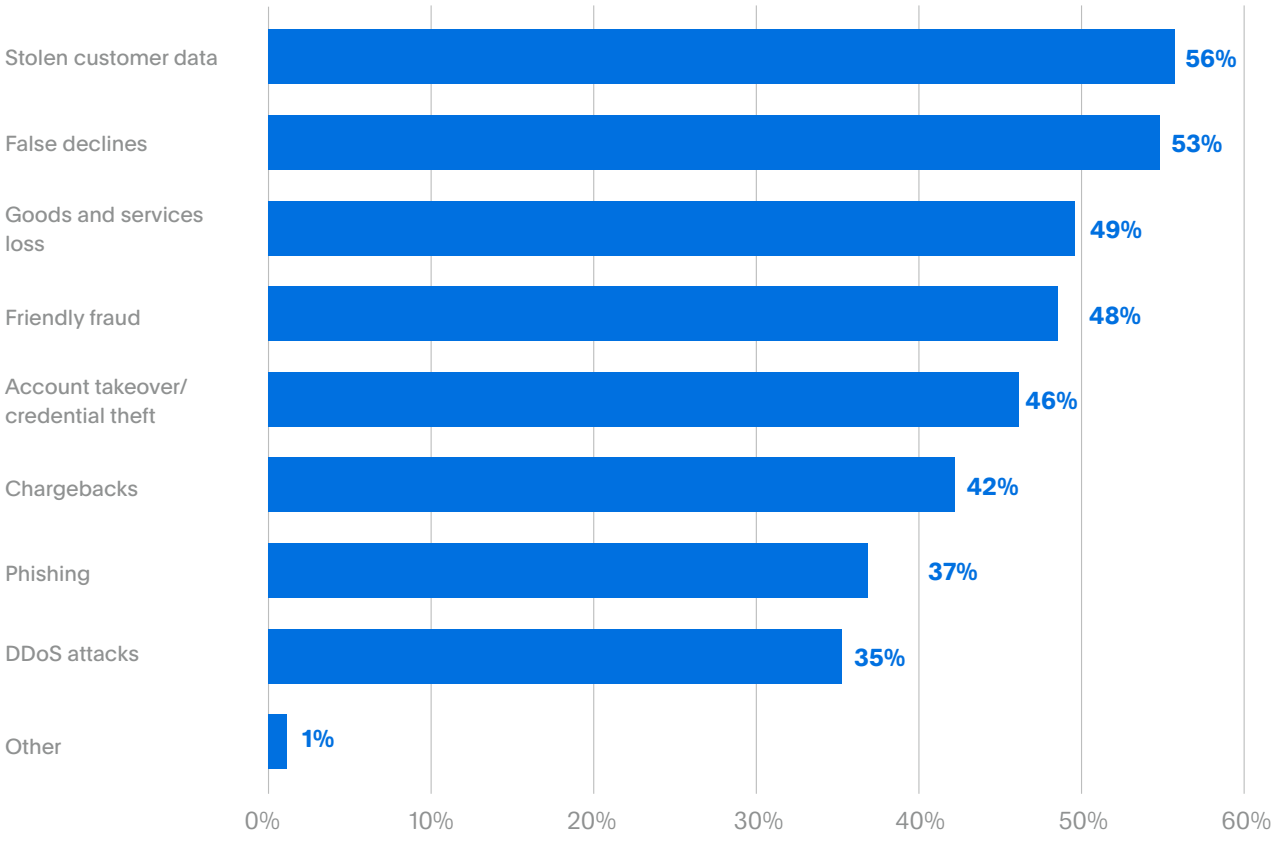
62% Customer information	**42%** Employee records	**26%** Research data
58% Financial information	**39%** Source code	**23%** Business correspondence
52% Intellectual property	**29%** Trade secrets	**21%** Product information
54% Payment data	**28%** Legal documents	**4%** Other

To minimize revenue losses, organizations should prioritize the protection of customer data. Figure 3 lists the most significant online payment risks. The biggest concern, according to 56% of respondents, is the theft of customer data due to the increasing sophistication of fraudsters.

This is followed by false declines (53% of respondents), which is defined as a legitimate transaction blocked by fraud prevention systems. This occurs when something about the transaction gets inaccurately flagged as fraudulent. This inaccurate flag occurs because there are several verifications put in place by an organization's system.

56% **of respondents say the biggest concern is the theft of customer data due to the increasing sophistication of fraudsters.**

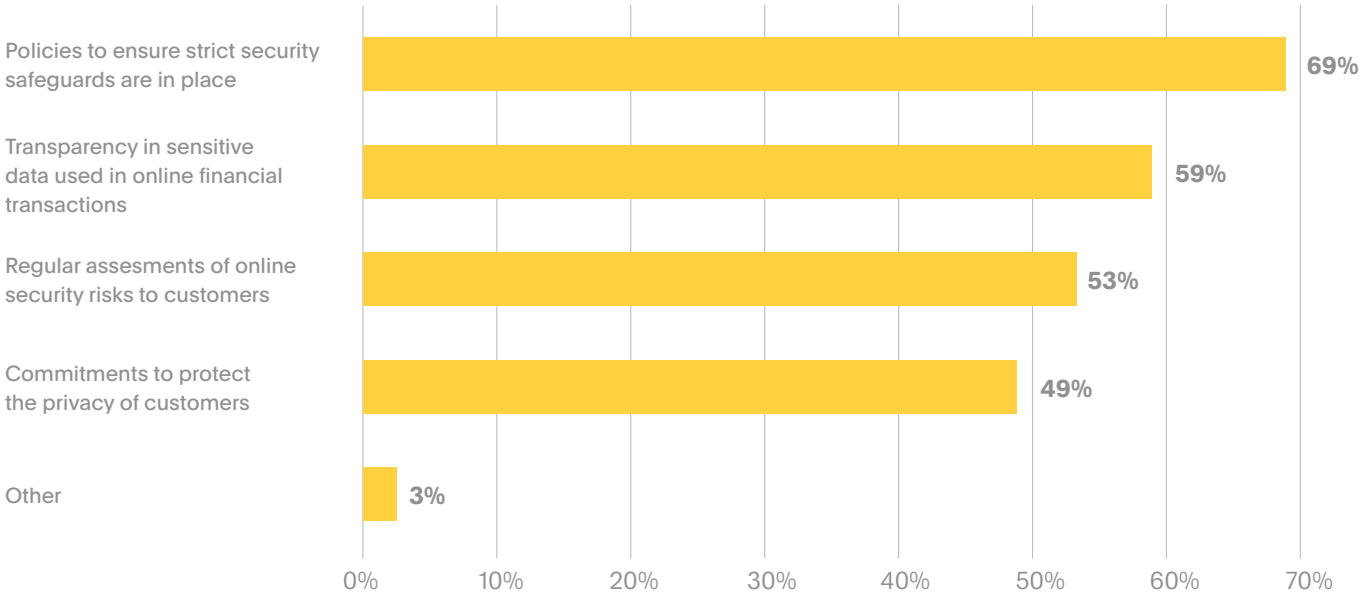
Figure 3. What are your organization's most significant payment risks?
More than one response permitted



To avoid customer turnover, organizations need to be considered trustworthy. According to Figure 4, the primary step taken to create and retain customers' trust in organizations' online transactions is to have policies to ensure strict security safeguards are in place (69% of respondents). This is followed by transparency in sensitive data used in online financial transactions (59% of respondents) and regular assessments of online security risks to customers (53% of respondents).

69% of respondents say the primary step taken to create and retain customers' trust in organizations' online transactions is to have policies to ensure strict security safeguards are in place.

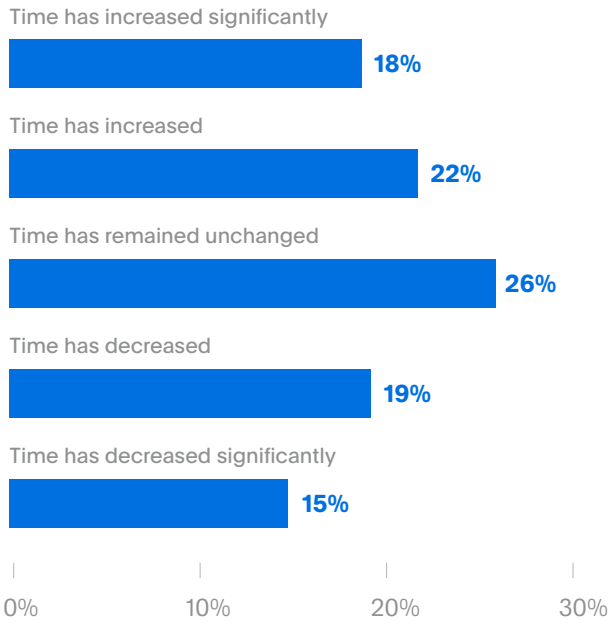
Figure 4. What steps does your organization take to create and retain trust in its online transactions?
More than one response permitted



Organizations are at great risk for the theft of customer data because of the inability to quickly respond to online fraud incidents. On average, organizations represented in this research have 8.78 million online transactions annually and of these an average of 29% or 2.5 million are compromised annually. Organizations, on average, spend 14 days to respond to an online fraud incident.

As shown in Figure 5, only 34% of respondents say the time to detect, contain and respond to an online fraud incident has decreased (19% of respondents) or decreased significantly (15% of respondents). As a result, organizations are at great risk for the theft of customer data.

Figure 5. In the past 12 months, how has the time to detect, contain and respond to an online fraud incident changed?

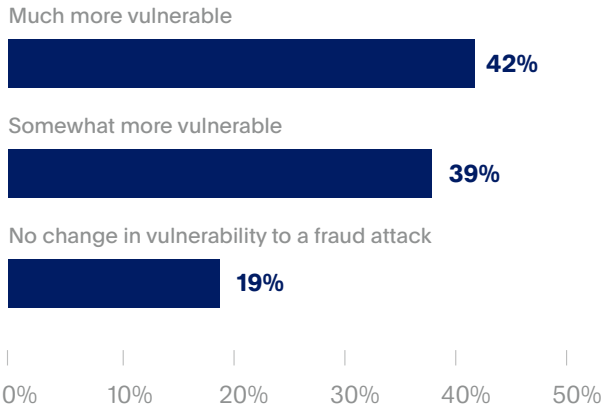


Digital transformation creates online fraud risks. 53% of respondents say they are familiar with their organizations' strategy for achieving digital transformation. According to Figure 6, 81% of respondents say their organizations are much more vulnerable (42%) or vulnerable (39%) to an online fraud attack due to digital transformation.

81%

of respondents say their organizations are much more vulnerable (42%) or vulnerable (39%) to an online fraud attack due to digital transformation.

Figure 6. Is your organization more vulnerable to an online fraud attack following digital transformation?

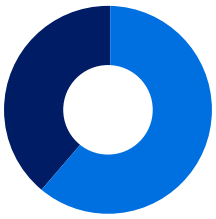


Organizations acknowledge the online fraud risks created by digital transformation. Respondents were asked to rate the concerns organizations have about online fraud attacks due to digital transformation on a scale of 1 = no concern/not likely to 10 = significant concern/very likely. Figure 7 presents the 7+ responses on the 10-point scale.

59% of respondents say their organizations are significantly concerned about having an online fraud incident caused by insecure digital transformation and 56% of respondents say it is very likely an online fraud attack will occur due to insecure digital transformation. These risks should encourage organizations to leverage advanced technologies, such as automation and AI, to detect online fraud.

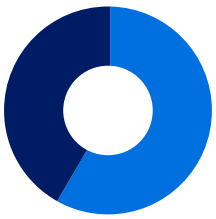
Figure 7. How risky are digital transformations that are insecure?

On a scale from 1 = no concern/not likely to 10 = significantly concerned/very likely, 7+ responses presented



59%

Concern about having an online fraud incident as a result of insecure digital transformation



56%

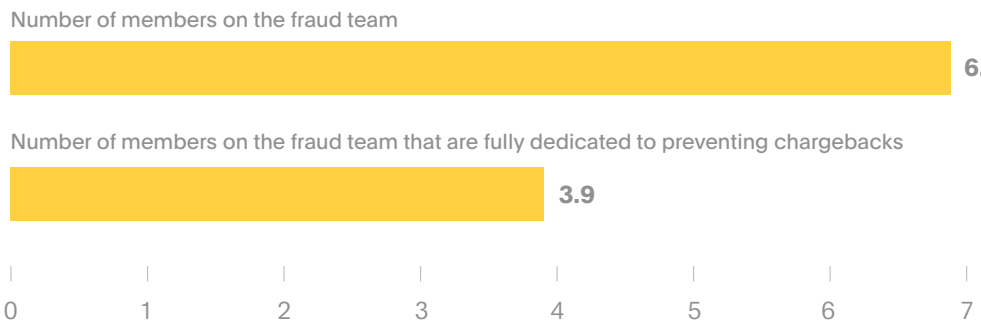
Likelihood that an online fraud attack will occur as a result of insecure digital transformation

The use of fraud teams to prevent and detect online fraud

Most organizations are using a team fully dedicated to detecting, responding and containing online fraud. 64% of respondents say their organizations have a team fully dedicated to the detection, response, and containment of online fraud. According to Figure 8, an average of 7 members are on the fraud team and in this team, 4 are fully dedicated to chargebacks. As defined in this research, chargeback fraud is the fraudulent request for a return or refund in the form of a chargeback. The customer disputes the transaction to regain the dollar amount while retaining the product or services rendered.

64% of respondents say their organizations have a team fully dedicated to the detection, response, and containment of online fraud.

Figure 8. How many members are on the fraud and chargeback teams?
Extrapolated values presented



Despite the use of fraud teams, only slightly more than half of respondents say their organizations are highly effective at reducing online fraud. Respondents were asked to rate the effectiveness of reducing and investigating online fraud on a scale from 1 = not effective to 10 = highly effective. Figure 9 presents the highly effective responses (7+ responses on the 10-point scale). 52% of respondents say their organizations are highly effective at reducing online fraud. Less than half (47%) of respondents say they are highly effective at investigating online fraud.

Less than half of respondents say they are highly effective at investigating online fraud.

Figure 9. Effectiveness in investigating and reducing online fraud

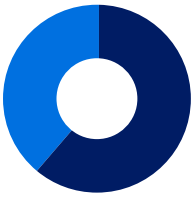
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented

The lack of collaboration between fraud and cybersecurity teams can be a barrier to minimizing online fraud. Respondents were asked to rate the level and importance of collaboration between fraud and cybersecurity teams on a scale of 1 = no collaboration achieved/collaboration not important to 10 = complete collaboration achieved/collaboration very important. Figure 10 presents the 7+ responses on the 10-point scale. While 60% of respondents say collaboration between the fraud and cybersecurity teams is very important, only 25% of respondents say complete collaboration has been achieved.

One possible reason for the difficulty in achieving collaboration is that important decisions are divided between the fraud function and IT security instead of being cohesive. Specifically, the fraud function directs the online fraud prevention strategies while IT security allocates the budget for technologies used to support these strategies.

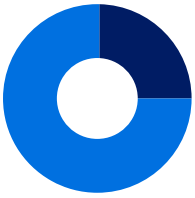
Figure 10. The state and importance of collaboration between the fraud and cybersecurity teams

On a scale of 1 = no collaboration/collaboration not important to 10 = complete collaboration/collaboration very important, 7+ responses presented



60%

Importance of collaboration between the fraud and cybersecurity team



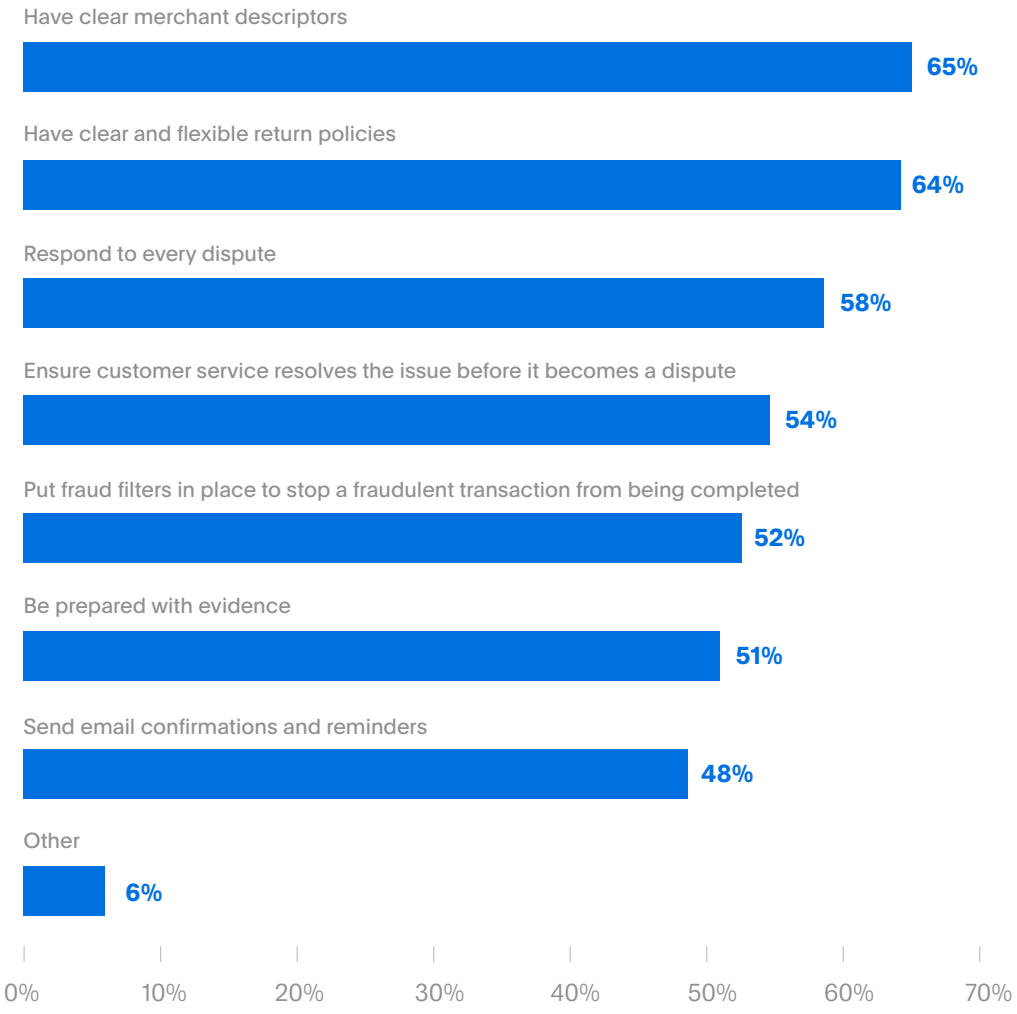
25%

Level of collaboration between the fraud and cybersecurity team

Organizations' approach to reducing chargeback fraud

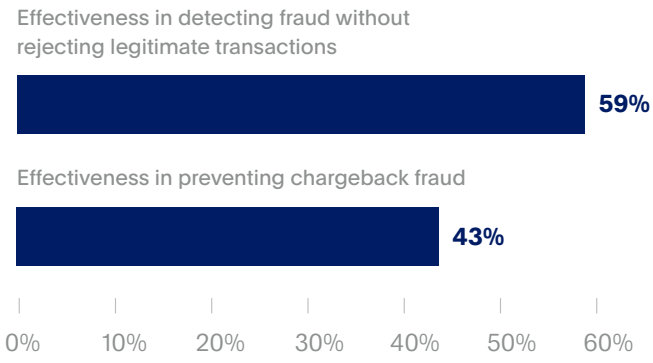
Chargeback fraud is a payment risk. As shown in Figure 11, the top two steps taken to prevent chargeback fraud are clear merchant descriptors (65% of respondents) followed by clear and flexible return policies (64% of respondents). Only slightly more than half (51%) of respondents say their organizations are prepared with evidence.

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



Organizations are more effective in dealing with false declines than preventing chargeback fraud. Respondents were asked to rate the effectiveness of dealing with false declines and chargeback fraud on a scale of 1 = not effective to 10 = highly effective. Figure 12 presents the highly effective responses (7+ on a 10-point scale). As shown, 59% of respondents say their organizations are highly effective in detecting fraud without rejecting legitimate transactions (false finds). However, only 43% of respondents say their organizations are highly effective in preventing chargeback fraud.

Figure 12. Effectiveness in preventing chargeback fraud and in detecting fraud without rejecting legitimate transactions
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented



43% of respondents say their organizations are highly effective in preventing chargeback fraud.

An average of 679 chargeback frauds are experienced each month. As shown in Figure 13, a monthly average of 31 hours is spent to investigate and respond to chargeback fraud. As discussed previously, 4 members of the fraud team are fully dedicated to preventing chargebacks.

Figure 13. The number of chargeback frauds each month and the time spent monthly to investigate and respond to chargeback fraud
Extrapolated values presented

679
Chargeback frauds experienced each month

31 hours
Time spent per month to investigate and respond to chargeback fraud

Securing online transactions with automation and other technologies

Most organizations are not prepared to prevent, detect, and respond to online fraud. According to Figure 14, only 42% of respondents say their organizations have the necessary in-house expertise to identify and prevent e-commerce fraud and only 44% of respondents say their organizations regularly assess the ability of their payments infrastructure to prevent and contain online financial fraud.

Further, online fraud strategies are not supportive of business initiatives and enablement. Less than half (46%) of respondents say their fraud security solutions and policies help balance security requirements with business enablement and only 44% of respondents say online fraud security strategies are aligned with business initiatives.

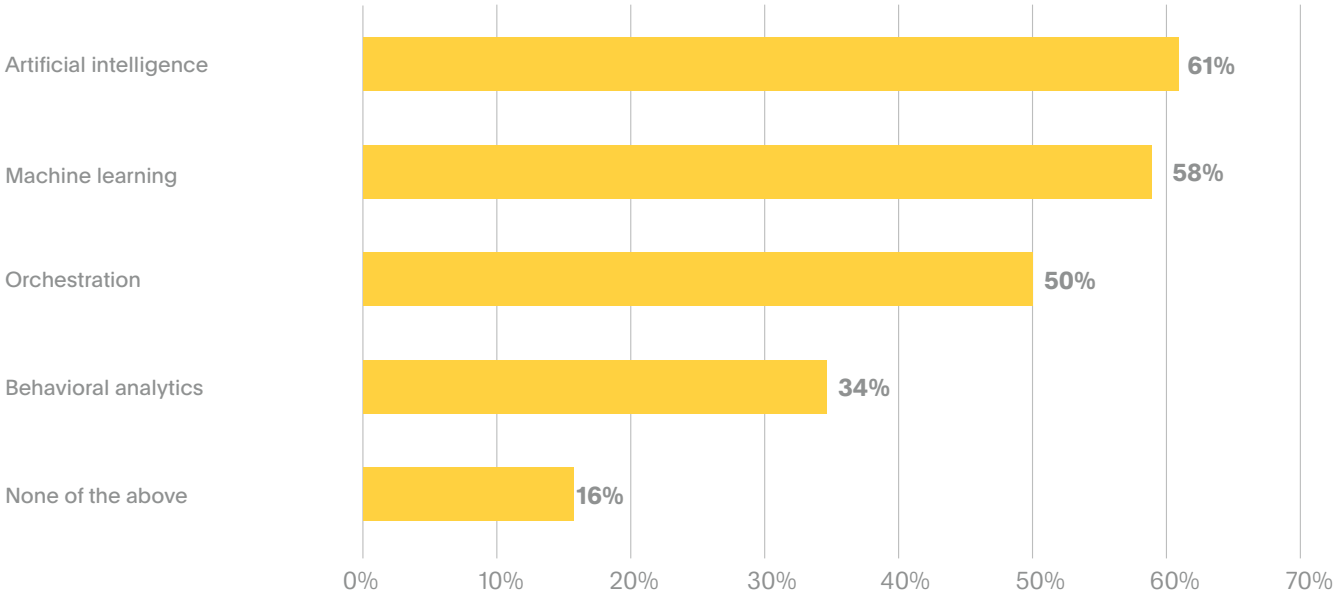
42% of respondents say their organizations have the necessary in-house expertise to identify and prevent e-commerce fraud.

Figure 14. Perceptions about online security *Strongly agree and agree responses presented*

AI and machine learning are the top technologies used to detect online fraud. 67% of respondents say their organizations use an automation layer to optimize fraud protection and authorization rates. Figure 15 lists technologies that organizations may use as part of their online fraud security practices and 53% of respondents who use these technologies say they are very essential.

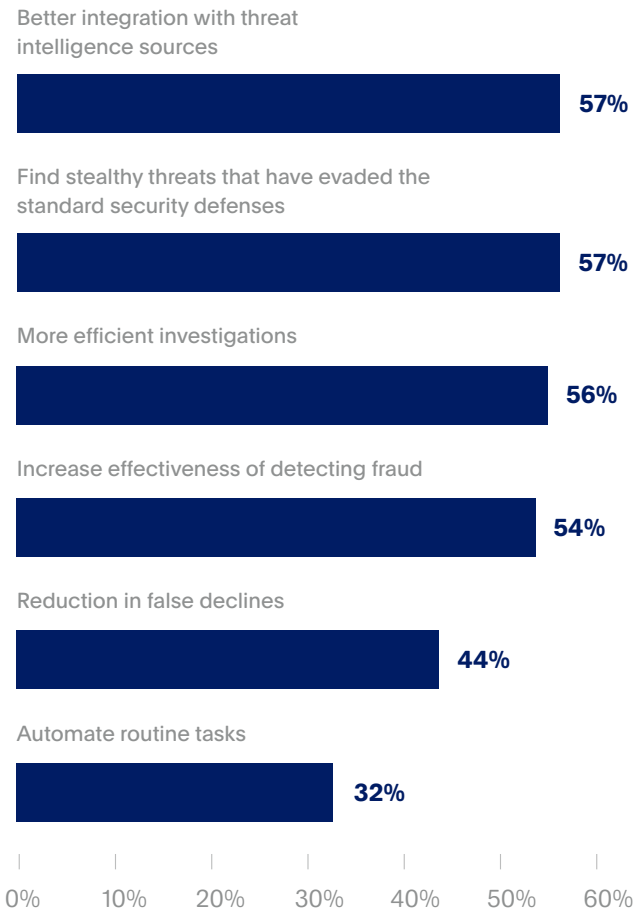
The most frequently used technologies are AI (61% of respondents), machine learning (58% of respondents) and orchestration (50% of respondents).

Figure 15. Does your organization use any of the following technologies to detect online fraud?
More than one response permitted



Of the organizations using these technologies, the two top benefits are better integration with threat intelligence sources and to find stealthy threats that have evaded the standard security defenses, as shown in Figure 16.

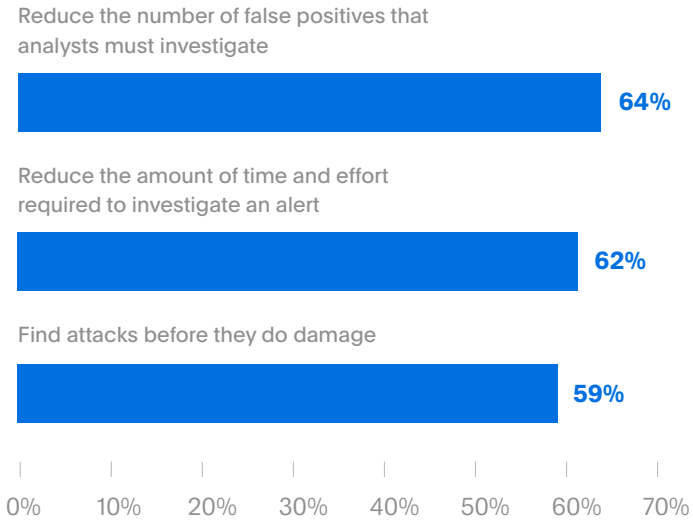
Figure 16. The top security benefits of using these technologies in fraud detection
Three responses permitted



The primary benefit of automation is greater efficiencies in the investigation of online fraud. As discussed, 67% of respondents say their organizations use an automation layer to optimize fraud protection and authorization rates. Respondents were asked to rate the importance of automation on a scale from 1 = low importance to 10 = highly important. Figure 17 presents the very and highly important responses (7+ on the 10-point scale).

As shown, most respondents are getting value out of automation. The number one benefit is the reduction in the number of false positives that analysts must investigate (64% of respondents) followed by reduction in the time and effort required to investigate an alert (62% of respondents). Automation is also considered helpful in finding attacks before they do damage (59% of respondents).

Figure 17. The benefits of automation 7+ responses
On a scale from 1 = low importance to 10 = highly important, 7+ responses permitted



Organizations' online compliance and governance practices

Compliance is not an important part of the organizations' online fraud prevention strategy. According to Figure 18, only 46% of respondents say achieving compliance with regulations is considered an important objective of anti-fraud efforts and only 44% of respondents say compliance with regulations is the minimum standard for achieving a strong security posture.

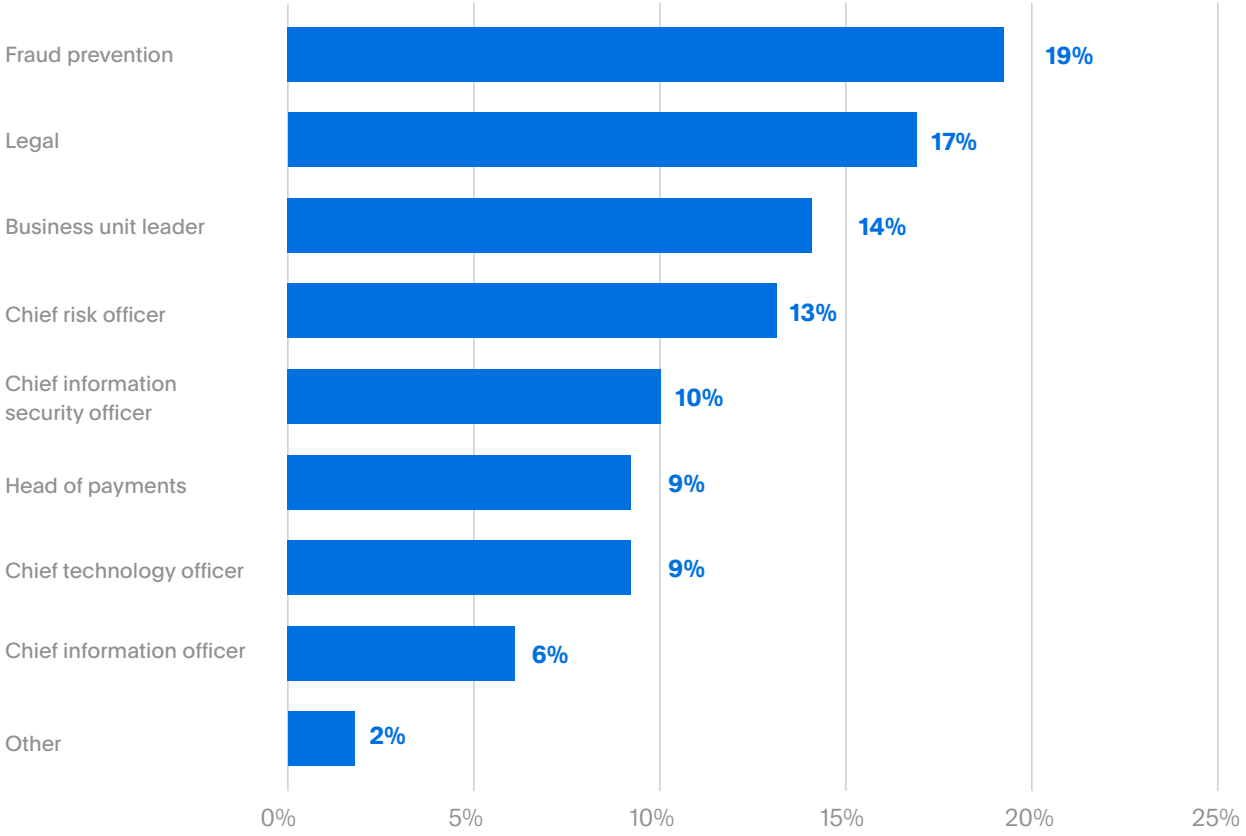
46% of respondents say achieving compliance with regulations is considered an important objective of anti-fraud efforts.

Figure 18. Perceptions about protection of online transactions *Strongly agree and Agree responses presented*

Fraud prevention, legal and the chief risk officer are most involved in making fraud prevention decisions. Figure 19 presents a list of functions that could be most involved in fraud prevention decisions. Almost half (49%) of respondents who are most involved in determining how best to secure online transactions without losing revenues are in fraud prevention, legal and the risk functions. In contrast, only 25% of IT and IT security are most involved in decision making.

Only 25% of IT and IT security are **most involved in decision making.**

Figure 19. Who is most involved in making decisions about fraud prevention in your organization?



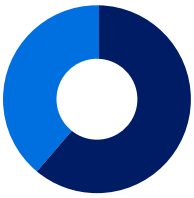
The impact of online fraud on revenues, cost, and budget

While most organizations are effective in preventing lost sales at the checkout, they struggle in balancing strong fraud protection with preferred payment methods. Respondents were asked to rate the effectiveness in preventing lost sales on a scale from 1 = not effective to 10 = highly effective.

Figure 20 presents the 7+ responses on the 10-point scale. 59% of respondents say their organizations are very or highly effective in keeping customer data current and preventing lost sales at the checkout. 57% of respondents say their organizations are very or highly effective in having both strong fraud protection and positive authorization rates.

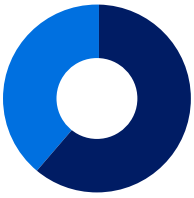
Figure 20. Effectiveness in preventing lost sales

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



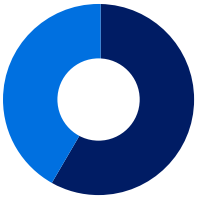
59%

Effectiveness in keeping customer data current



59%

Effectiveness in preventing lost sales at the checkout



57%

Effectiveness in striking a balance between strong fraud protection and positive authorization rates

Customer sales are frequently lost due to transactions being declined. Respondents were asked to rate the frequency of lost sales on a scale from 1 = not frequent to 10 = very frequently. Figure 21 shows the frequent and very frequent responses. While less than half (47%) of respondents have frequently abandoned a shopping cart when not having their preferred payment method available, transactions are being frequently declined (56% of respondents).

Figure 21. Frequency of lost sales

On a scale from 1 = not frequently to 10 = very frequently, 7+ responses presented

According to Figure 22, 46% of respondents say their organizations are allocating more than $500,000 to online fraud prevention.

Figure 22. Approximately, what range best defines your organization's 2022 online fraud budget?

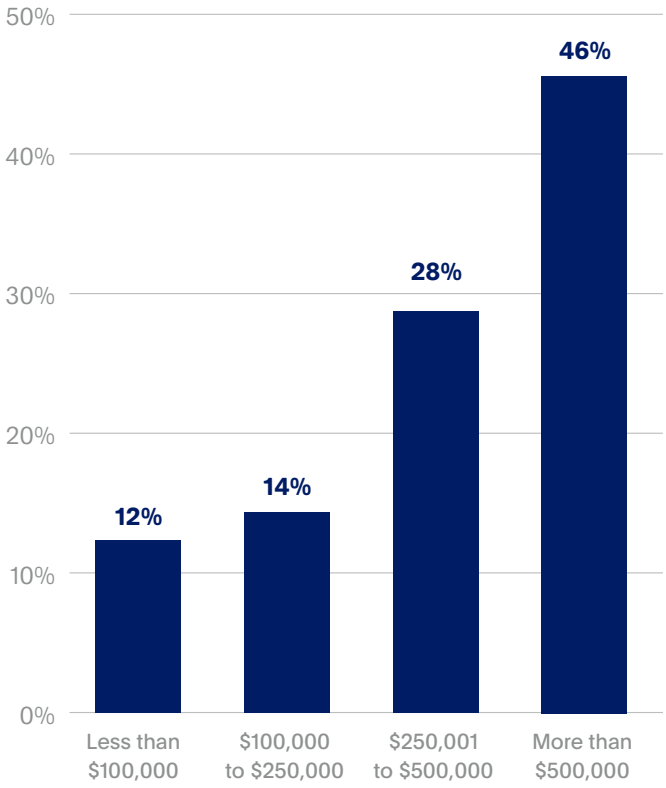


Table 1 provides seven cost categories of online fraud. As shown, most of the budget is allocated to operational costs (23%), chargeback fraud (16%) and customer attrition (15%).

Table 1. Allocation of the budget to seven cost categories of online fraud

Cost categories	Percentage distribution
Operational costs	23%
Chargeback fraud	16%
Customer attrition	15%
Customer retention	13%
Loss of business relationships	12%
Legal and regulatory costs	11%
Reputation and brand damage	10%
Total	**100%**

Methods

A sampling frame of 76,094 individuals who are involved at some level in deciding which tools/ solutions their organizations use for accepting payments and how it completes credit card and debit card transactions from customers or risk solutions were selected as participants to this survey. Table 2 shows 4,000 total returns. Screening and reliability checks required the removal of 261 surveys. Our final sample consisted of 3,749 surveys or a 4.9% response.

Table 2. Sample response

	Freq	Pct%
Sampling frame	76,094	100.0%
Total returns	4,000	5.3%
Rejected or screened surveys	261	0.3%
Final sample	3,739	4.9%

Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (61%) of respondents are at or above the supervisory levels. The largest category at 18% of respondents is manager.

Pie Chart 1. Current position within the organization

- 6% Senior Executive
- 7% Vice President
- 14% Director
- 18% Manager
- 16% Supervisor
- 17% Technician/Analyst
- 12% Staff
- 7% Contractor
- 3% Other

According to Pie Chart 2, 17% of respondents are located within corporate IT. This is followed by IT security (15% of respondents), internal audit (11% of respondents), risk management (10% of respondents), fraud prevention (10% of respondents), and payment processing (10% of respondents).

Pie Chart 2. Respondents' primary department within the organization

- 17% Corporate IT
- 15% IT Security
- 11% Internal Audit
- 10% Risk Management
- 10% Fraud Prevention
- 10% Payment Processing
- 9% Compliance
- 8% Supply Chain
- 7% Finance & Accounting
- 3% Other

Caveats to this study

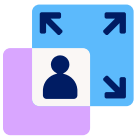
There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

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 involved in deciding which tools/solutions their organizations use for accepting payments. 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.

Appendix with the detailed audited finding

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in June 2022.

Survey response

Total sampling frame	76,094
Total survey returns	4,000
Rejected surveys	261
Final sample	3,739
Response rate	3.80%

S1.

What is your role in deciding which tools/solutions your organization uses for accepting payments and how it completes credit card and debit card transactions from customers or risk solutions?

The sole decision maker	29%
A key decision maker	31%
An influential decision maker	22%
Some influence over the decision	17%
No influence (Stop)	0%
Total	100%

S2.

What percentage of your organization's total sales are from online transactions?

Less than 20%	0%
20% to 30%	42%
31% to 50%	30%
More than 50%	28%
Total	100%

S3.

Approximately, what was your organization's annual revenue in 2021?

Less than $20,000,000 (Stop)	0%
$20,000,000 to $30,000,000	45%
$30,000,001 to $50,000,000	26%
$50,000,000 to $100,000,000	19%
$100,000,001 to $250,000,000	14%
$250,000,001 to $500,000,000	10%
More than $500,000,000	6%
Total	100%

S4.

What best describes your organization's industry focus? Please select one choice only.

E-commerce	8%
Online education	7%
Entertainment & media	9%
Financial services	11%
Gaming	9%
Grocery (food services)	17%
Hospitality	17%
Insurance	10%
Retailers	8%
Travel	5%
None of the above (Stop)	0%
Total	100%

Part 2. Attributions

Please rate each one of the following statements using the scale provided below each item. Strongly Agree and Agree response combined.

Q1a. Our organization makes it a priority to protect online financial transactions.	48%
Q1b My organization's leadership is willing to accept revenue losses because they believe the cost of protection outweighs the cost of dealing with losses.	39%
Q1c. My organization regularly assesses the ability of its payments infrastructure to prevent and contain online financial fraud.	44%
Q1d. My organization has the necessary in-house expertise to identify and prevent e-commerce fraud.	42%
Q1e. Our online fraud security solutions and policies help balance security requirements with business enablement.	46%
Q1f. Our organization implements online fraud security strategies that align with its business initiatives.	44%
Q1g. Achieving compliance with such regulations as 3DS Security Protocol, PSD2, PCI-DSS and other government regulations is an important objective of our organization's anti-fraud efforts.	46%
Q1h. Our organization considers compliance with regulations as the minimum standard for achieving a strong security posture.	44%

Q2a.

How effective is your organization in investigating online fraud on a scale from 1 = not effective to 10 = highly effective?

1 to 2	8%
3 to 4	14%
5 to 6	25%
7 to 8	28%
9 to 10	24%
Total	100%
Extrapolated value	6.41

Q2b.

How effective is your organization in reducing online fraud on a scale from 1 = not effective to 10 = highly effective?

1 to 2	12%
3 to 4	17%
5 to 6	24%
7 to 8	26%
9 to 10	21%
Total	100%
Extrapolated value	6.03

Q2c.

How effective is your organization in achieving compliance with IT security and privacy regulations on a scale from 1 = not effective to 10 = highly effective?

1 to 2	15%
3 to 4	18%
5 to 6	26%
7 to 8	22%
9 to 10	19%
Total	100%
Extrapolated value	5.72

Part 3. Security of online transactions

Q3.

What are the primary challenges to mitigating online financial fraud? Please select all the top three challenges.

Lack of budget	30%
Lack of in-house expertise	42%
Lack of leadership	33%
Our organization does not have programs or policies for dealing with online financial fraud	33%
Not considered a priority	43%
Our organization does not have the right technologies to mitigate online financial fraud	55%
The increasing sophistication of fraudsters	63%
Other (please specify)	1%
Total	300%

Q4.

What types of data are most at risk in your organization? Please select all that apply.

Employee records	42%
Intellectual property	52%
Business correspondence	23%
Legal documents	28%
Customer information	62%
Research data	26%
Payment data	54%
Trade secrets	29%
Source code	39%
Financial information	58%
Product information	21%
Other (please specify)	4%
Total	437%

Q5.

What are your organization's most significant payment risks? Please select all that apply.

Stolen customer data	56%
False declines	53%
Goods and services loss	49%
Friendly fraud	48%
Chargebacks	42%
Phishing	37%
DDoS attacks	35%
Account takeover/credential theft	46%
Other	1%
Total	367%

Q6.

Who is most involved in making decisions about fraud prevention in your organization? Please check one choice only.

Business unit leader	14%
Chief information officer (CIO)	6%
Chief technology officer (CTO)	9%
Chief risk officer (CRO)	13%
Chief information security officer (CISO)	10%
Fraud prevention	19%
Head of payments	9%
Legal	17%
Other (please specify)	2%
Total	100%

Q7.

What steps does your organization take to create and retain trust in its online transactions? Please select all that apply.

Transparency in sensitive data used in online financial transactions	59%
Commitments to protect the privacy of customers	49%
Policies to ensure strict security safeguards are in place	69%
Regular assessments online security risks to customers	53%
Other (please specify)	3%
Total	234%

Q8a.

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

Yes	64%
No (please skip to Q9a)	36%
Total	100%

Q8b.
If yes, how many members are on the fraud team?

1 to 3	22%
4 to 5	27%
6 to 10	25%
More than 10	26%
Total	100%
Extrapolated value	6.80

Q8c.
If yes, how many members of the fraud team are fully dedicated to preventing chargebacks?

None	7%
1 to 2	11%
3 to 4	27%
More than 4	56%
Total	100%
Extrapolated value	3.88

Q9a.
How much collaboration occurs between the fraud and cybersecurity team on a scale of 1 = no collaboration to 10 = complete collaboration?

1 to 2	28%
3 to 4	29%
5 to 6	17%
7 to 8	16%
9 to 10	9%
Total	100%
Extrapolated value	4.49

Q9b.
How important is collaboration between the fraud and cybersecurity team on a scale of 1 = not important to 10 = very important?

1 to 2	7%
3 to 4	13%
5 to 6	20%
7 to 8	27%
9 to 10	33%
Total	100%
Extrapolated value	6.85

Q10.
What steps are taken to prevent chargeback fraud? Please check all that apply.

Be prepared with evidence	51%
Ensure customer service resolves the issue before it becomes a dispute	54%
Have clear and flexible return policies	64%
Have clear merchant descriptors	65%
Put fraud filters in place to stop a fraudulent transaction from being completed	52%
Respond to every dispute	58%
Send email confirmations and reminders	48%
Other (please specify)	6%
Total	398%

Q11.
How effective is your organization in preventing chargeback fraud on a scale from 1 = not effective to 10 = highly effective?

1 to 2	16%
3 to 4	17%
5 to 6	23%
7 to 8	23%
9 to 10	20%
Total	100%
Extrapolated value	5.78

Q12.
Approximately, how many chargeback frauds does your organization experience each month?

5 to 50	11%
51 to 100	17%
101 to 1,000	30%
More than 1,000	41%
Total	100%
Extrapolated value	679

Q13a.

On average, approximately how much time is spent monthly to investigate and respond to chargeback fraud?

Less than 5 hours	6%
5 to 10 hours	12%
11 to 25 hours	18%
26 to 50 hours	29%
More than 50 hours	34%
Total	100%
Extrapolated value	31.11

Q13b.

On average, approximately how many staff are involved monthly in investigating and responding to chargeback fraud?

Less than 3	15%
3 to 5	22%
6 to 10	32%
More than 10	30%
Total	100%
Extrapolated value	7.51

Q14.

How effective is your organization in detecting fraud without rejecting legitimate transactions 1 = not effective to 10 = highly effective?

1 to 2	9%
3 to 4	14%
5 to 6	18%
7 to 8	27%
9 to 10	32%
Total	100%
Extrapolated value	6.68

Q15.

Does your organization use an automation layer to optimize fraud protection and authorization rates?

Yes	67%
No	33%
Total	100%

Q16.

Does your organization use any of the following technologies to detect online fraud? Please select all that apply.

Artificial intelligence	61%
Machine learning	58%
Orchestration	50%
Behavioral analytics	34%
None of the above (Please skip to Q20)	16%
Total	218%

Q17.

If your organization uses any of these technologies, how essential are they to detecting online fraud incidents on a scale from 1 = not essential to 10 = very essential?

1 to 2	15%
3 to 4	12%
5 to 6	20%
7 to 8	30%
9 to 10	23%
Total	100%

Q18.

What are the top three key security benefits of using these technologies in fraud detection? Please select your top three choices.

Automate routine tasks	32%
Find stealthy threats that have evaded the standard security defenses	57%
Increase effectiveness of detecting fraud	54%
Better integration with threat intelligence sources	57%
More efficient investigations	56%
Reduction in false declines	44%
Total	300%

Q19.
Using the following ten-point scale, please rate the importance of the following three benefits of automation to achieving a more efficient and effective online security posture from 1 = low importance to 10 = highly important.

Q19a.
Reduce the number of false positives that analysts must investigate

1 to 2	7%
3 to 4	12%
5 to 6	17%
7 to 8	26%
9 to 10	38%
Total	100%
Extrapolated value	7.03

Q19b.
Reduce the amount of time and effort required to investigate an alert

1 to 2	8%
3 to 4	11%
5 to 6	19%
7 to 8	28%
9 to 10	34%
Total	100%
Extrapolated value	6.88

Q19c.
Find attacks before they do damage

1 to 2	9%
3 to 4	14%
5 to 6	18%
7 to 8	27%
9 to 10	32%
Total	100%
Extrapolated value	6.68

Q20.
In the past 12 months, how has the time to detect, contain and respond to an online fraud incident changed?

Time has increased significantly	18%
Time has increased	22%
Time has remained unchanged	26%
Time has decreased	19%
Time has decreased significantly	15%
Total	100%

Q21.
What is the average time (days) to respond to an online fraud incident?

Less than 1 day	9%
1 day to 2 days	21%
3 days to 1 week	24%
2 weeks to 1 month	26%
More than 1 month	20%
Total	100%
Extrapolated value (days)	13.7

Q22a.
Does your organization have a dedicated incident response plan for fraud incidents?

Yes	64%
No	36%
Total	100%

Q22b.
If yes, does the plan include proactive steps to respond to online fraud incidents?

Yes	58%
No	42%
Total	100%

Q23.
Are you familiar with your organization's strategy for achieving digital transformation?

Yes	53%
No (please skip to Q27)	47%
Total	100%

Q24.
Is your organization more vulnerable to an online fraud attack following digital transformation?

Yes, much more vulnerable	42%
Yes, somewhat more vulnerable	39%
No change in vulnerability to a fraud attack	19%
Total	100%

Q25.
How concerned is your organization about having an online fraud incident as a result of insecure digital transformation on a scale from 1 = no concern to 10 = significantly concerned?

1 to 2	9%
3 to 4	14%
5 to 6	18%
7 to 8	27%
9 to 10	32%
Total	100%
Extrapolated value	6.68

Q26.
How likely is it that your organization had an online fraud attack as a result of insecure digital transformation on a scale from 1 = not likely to very likely?

1 to 2	9%
3 to 4	15%
5 to 6	20%
7 to 8	27%
9 to 10	29%
Total	100%
Extrapolated value	6.55

Q27.
How effective is your organization in preventing lost sales at the checkout on a scale from 1 = not effective to 10 = highly effective?

1 to 2	9%
3 to 4	14%
5 to6	18%
7 to 8	27%
9 to 10	32%
Total	100%
Extrapolated value	6.68

Q28.
How effective is your organization in keeping customer data current on a scale from 1 = not effective to 10 = highly effective?

1 to 2	9%
3 to 4	14%
5 to 6	18%
7 to 8	27%
9 to 10	32%
Total	100%
Extrapolated value	6.68

Q29.
How effective is your organization in striking a balance between strong fraud protection and positive authorization rates on a scale from 1 = not effective to 10 = highly effective?

1 to 2	9%
3 to 4	14%
5 to 6	20%
7 to 8	27%
9 to10	30%
Total	100%
Extrapolated value	6.60

Q30.
How frequently do your online customers leave without placing an item in the shopping cart on a scale from 1 = not frequently to 10 = very frequently.

1 to 2	9%
3 to 4	14%
5 to 6	18%
7 to 8	29%
9 to 10	30%
Total	100%
Extrapolated value	6.64

Q31.
How frequently do your online customers abandon a shopping cart when their preferred payment method is unavailable on a scale from 1 = not frequently to 10 = very frequently.

1 to 2	9%
3 to 4	14%
5 to 6	30%
7 to 8	27%
9 to 10	20%
Total	100%
Extrapolated value	6.20

Q32.
How frequently do your online customers experience at least one of their transactions being declined on a scale from 1 = not frequently to 10 = very frequently.

1 to 2	9%
3 to 4	10%
5 to 6	25%
7 to 8	29%
9 to 10	27%
Total	100%
Extrapolated value	7.40

Part 4. The cost of fraud

Q33.
How many online transactions does your organization have annually?

Less than 10,000	7%
10,000 to 25,000	12%
25,001 to 50,000	8%
50,001 to 100,000	10%
101,000 to 250,000	8%
251,000 to 500,000	8%
501,000 to 1,000,000	9%
1,001,000 to 5,000,000	11%
5,001,000 to 10,000,000	11%
10,001,000 to 50,000,000	11%
50,001,000 to 100,000,000	5%
More than 100,000,000	0%
Total	100%

Q34.
On average, what percentage of these online transactions are compromised annually?

Less than 10%	24%
10% to 25%	28%
26% to 50%	26%
More than 50%	23%
Total	100%
Extrapolated value	29%

Q35a.
Does your organization calculate the revenue lost due to online fraudulent transactions?

Yes	49%
No	51%
Total	100%

Q35b.
If yes, on average how much revenue is lost per year due to online fraudulent transactions?

Less than $50,000	2%
$50,000 to $100,000	2%
$101,000 to $250,000	5%
$251,000 to $500,000	7%
$501,000 to $1,000,000	8%
$1,001,000 to $1,500,000	14%
$1,501,000 to $2,000,000	13%
$2,001,000 to $5,000,000	22%
$5,001,000 to $10,000,000	14%
More than $10,000,000	12%
Total	100%

Q36.
The following table provides seven cost categories of online fraud, including chargeback fraud. Please allocate all 100 points to provide the relative distribution of each cost category. Please keep in mind that the total points must equal 100.

Operational costs	23.00
Legal and regulatory costs	11.00
Reputation and brand damage	10.00
Customer attrition	15.00
Customer retention	13.00
Loss of business relationships	12.00
Chargeback fraud	16.00
Total points	100.00

Part 5. Budget

Q37.
Where does the budget reside for funding the prevention, response to and the containment of an online fraud incident?

IT	40%
IT security	26%
Compliance	19%
Finance	12%
Other	3%
Total	100%

Q38.
Approximately, what range best defines your organization's 2022 online fraud budget?

Less than $100,000	12%
$100,000 to $250,000	14%
$250,001 to $500,000	28%
More than $500,000	46%
Total	100%

Part 6. Your role & organization characteristics

D1.
What organizational level best describes your current position?

Senior Executive	6%
Vice president	7%
Director	14%
Manager	18%
Supervisor	16%
Technician/Analyst	17%
Staff	12%
Contractor	7%
Other	3%
Total	100%

D2.
What best describes your primary department in the organization?

Compliance	9%
Corporate IT	17%
Finance & accounting	7%
Fraud prevention	10%
Internal audit	11%
IT security	15%
Payment processing	10%
Risk management	10%
Supply chain	8%
Other	3%
Total	100%

PayPal.com