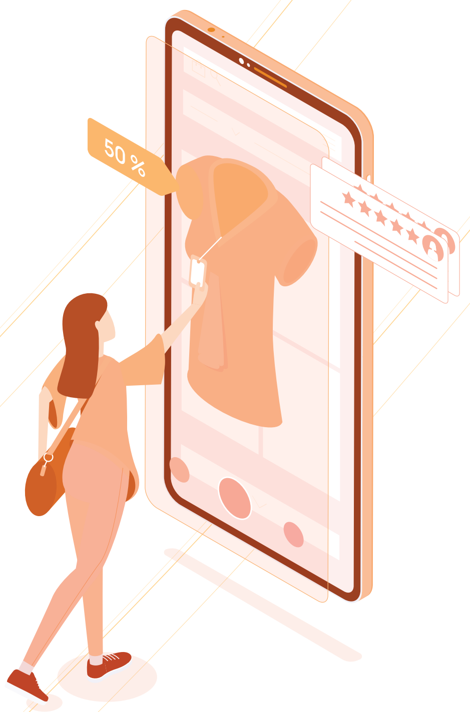
clearsale

False Declines Industry Report

Balancing Revenue, Fraud Prevention, and the E-Commerce Customer Experience.



Online merchants know that e-commerce fraud poses a threat to their profits.

They tend to be less aware of – and certainly less prepared for – the risk that false declines poses to profits and the customer experience their online store delivers.

As consumers increasingly use their digital devices to make online purchases, merchants find themselves struggling to find the right balance between robust fraud protection and a frictionless checkout experience.

Achieving this balance isn't easy, but it's critical to the success of every online store.

A new report commissioned by ClearSale and researched by the Aite Group – "The E-Commerce Conundrum: Balancing False Declines and Fraud Prevention" – provides new insights into how online merchants today are navigating this challenge.

Key takeaways from our report on false declines:

$443 billion

in revenue lost to false declines

- Losses due to e-commerce fraud are projected to reach $6.4 billion by 2021. But losses due to false declines are projected to reach $443 billion by 2021 – nearly 70x more than losses from fraud itself.
- 62% of online merchants have seen false decline rates increase over the past two years.
- Automatically declining suspicious transactions may be the reason behind high false decline rates.
- Customers become unhappy when their orders are incorrectly declined, and this dissatisfaction can hurt sales over the long term.

62% of merchants

say their false decline rates are increasing

- In competitive markets, a frictionless buyer experience can be a key differentiator for savvy merchants. The challenge is to balance customer experience with efficient fraud prevention.
- Most merchants understand the need to combine automated decisions with manual reviews. But there's an opportunity to dramatically improve the artificial intelligence used to send orders to be manually reviewed.
- Merchants are carefully implementing fraud prevention strategies – but these strategies are not lowering their chargeback rates. Instead, they are harming the customer experience.

Our research uncovered interesting insights into how merchants are working to prevent fraud, reduce false declines, and improve their overall customer experience. Read on to learn more.

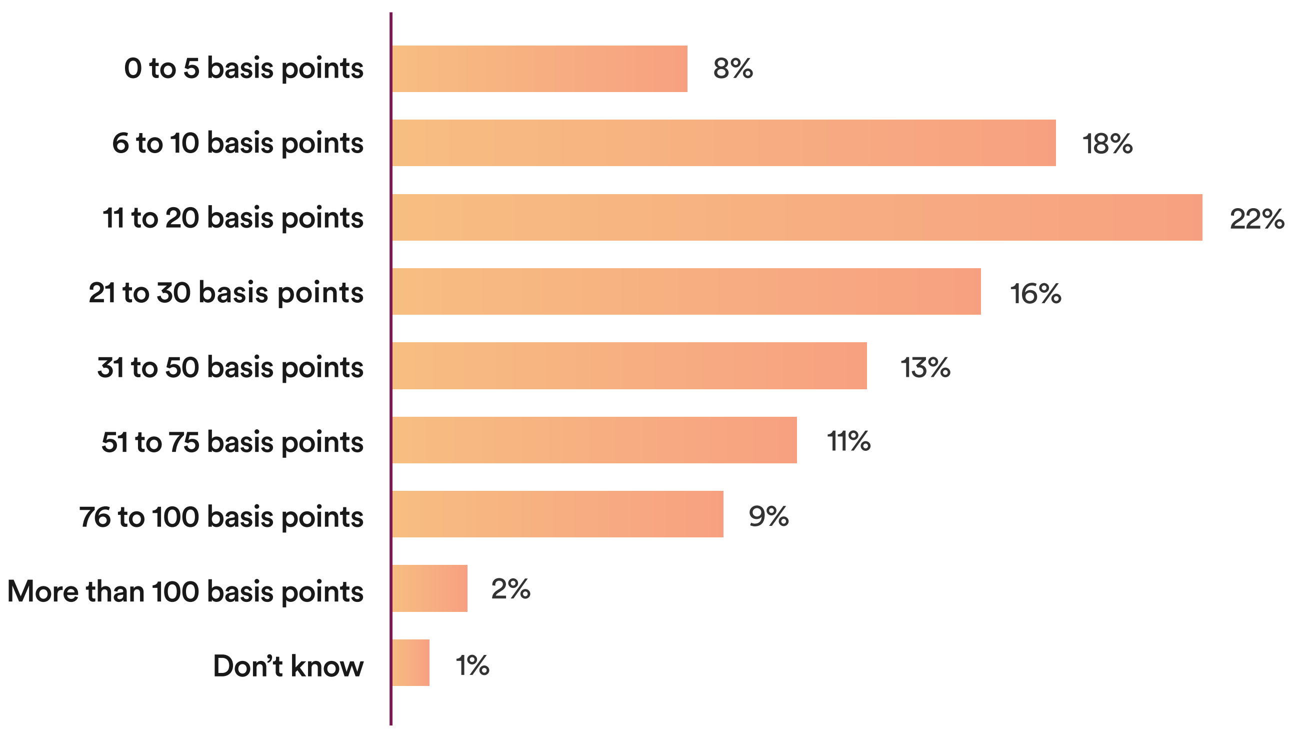
Contents

The Rise of E-Commerce Fraud

Yes, e-commerce fraud attacks are more and more common – both domestically and internationally. In fact, almost all of the merchants we surveyed reported at least some level of attempted fraud in 2018, and 22% said these fraud attacks exceeded 0.51% of their company's revenue.

22% of merchants experienced attempted fraud exceeding 0.51% of their company's revenue

Q: As a % of your company's revenue, what was the % of attempted fraud in 2018?



Organized crime rings are likely behind much of this fraud activity. Because the kingpins of these crime rings are seldom caught, there is little to prevent them from continuing to escalate their coordinated attacks.

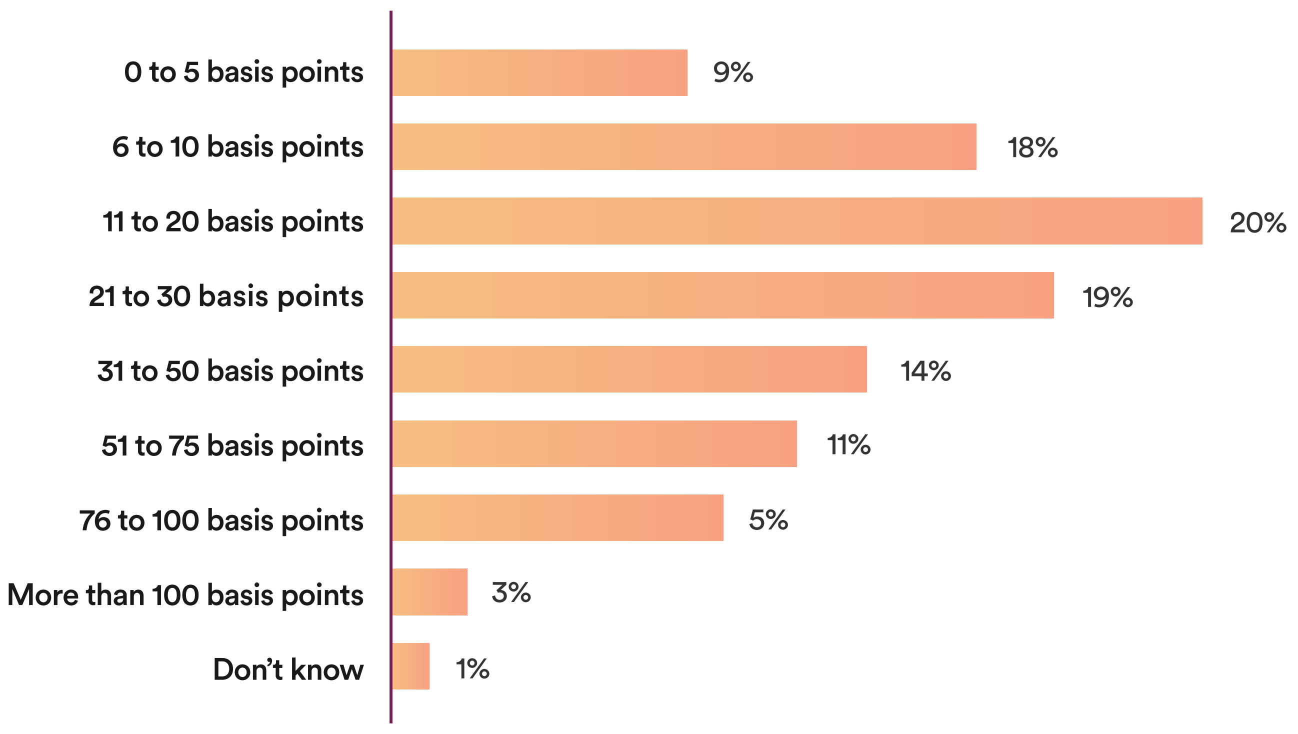
Rising fraud levels underscore the important of implementing robust fraud controls. This is especially true for merchants who have no idea how often they've been a target of fraud attacks.

Fraudulent Chargebacks Contribute to Revenue Losses

Losses caused by fraudulent chargebacks are a major contributor to fraud losses, with 19% of merchants surveyed reporting losses to fraudulent chargebacks costing more than .5% of revenue in 2018.

19% of merchants experienced fraudulent chargeback losses exceeding 0.5% of their company's revenue

Q: What were your losses to fraudulent chargebacks as a % of revenue in 2018?

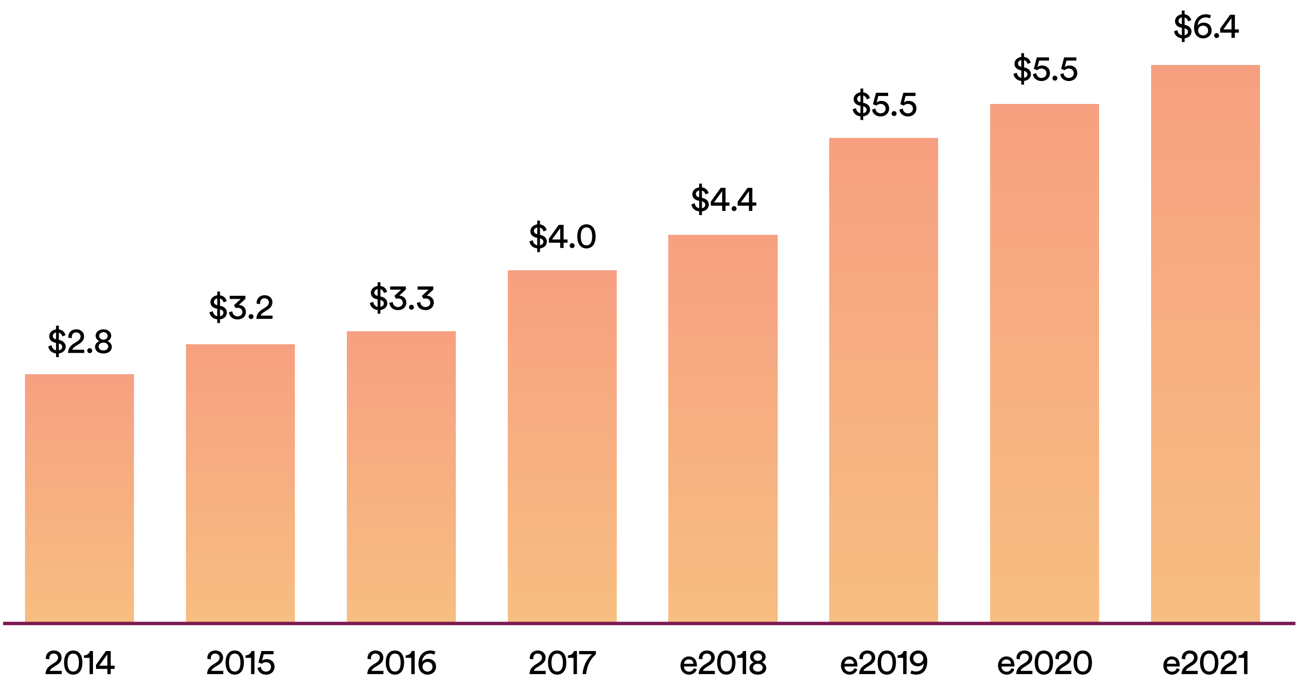


CNP Fraud Contributes to Revenue Losses

Despite the expectation that fraud would decrease in the wake of the global EMV implementation, the opposite has occurred. Card-not-present (CNP) fraud has escalated rapidly and is expected to top $6.4 billion in the United States by 2021.

CNP fraud will reach $6.4 billion in the US by 2021

Projected CNP Fraud Losses (in US$ Billions):



Top Fraud Prevention Strategies

When developing a fraud prevention strategy, the first decision a merchant must make is whether to build an in-house fraud prevention team or leverage a third-party fraud prevention provider.

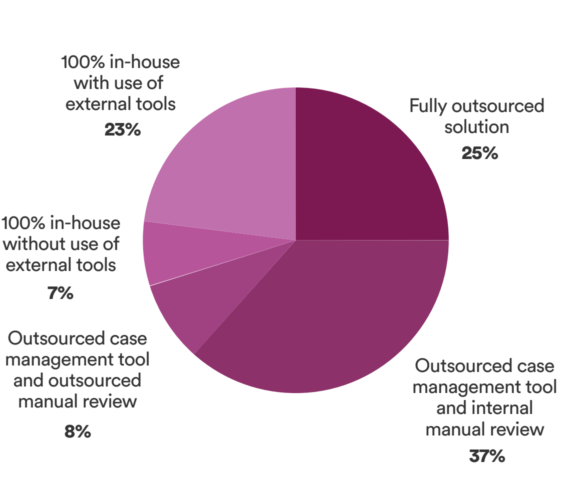
In-House or Outsourced Fraud Prevention?

Our study revealed a market trend towards outsourcing. Only 7% of merchants say they manage fraud prevention entirely in-house, with no outsourcing and no use of external tools.

This is notable because **five years ago, fewer than 5% of merchants outsourced their CNP fraud prevention.**

Today, 25% of merchants completely outsource their CNP fraud prevention

Q: Which of the following describes how your company handles CNP fraud prevention?

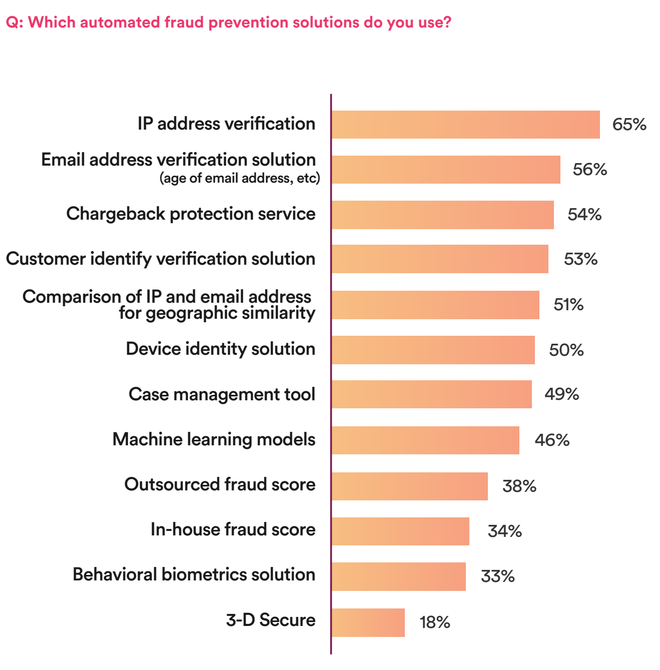


Automated Fraud Prevention Tactics

For those merchants who choose to partner with a third party, many of the solutions available involve automated processes:

Automated Tactic	Description
IP address verification	Examines the IP address to determine geographic location.
Email address verification	Determines the age of the email address and velocity of use and performs other tests.
Chargeback protection service	Guarantee service that shifts liability for chargebacks from the merchant to the solution provider.
Customer identity verification	Checks various data elements to third-party databases to determine whether a customer is who they claim to be.
Comparison of IP and email address for geographic similarity	Determines whether the IP address and email address originate from the same geographical location.
Device identity	Matches the identity of the device to one previously used by a returning customer.
Case management tool	Back-office tool used for manual review and potential charge-offs; can match customer details to determine if prior incidents have occurred with the customer.
Machine learning models	Analytic models trained to detect various types of suspicious activity.
Outsourced fraud score	Fraud score based on results from several solutions computed by an outside supplier.
In-house fraud score	Fraud score based on results from several fraud solutions computed by internal algorithms.
Behavioral biometrics	Used to detect bot or fraudster behavior and to match specific pattern of interaction with device as previously experienced by returning customer risk and issuer's method of authentication.
3D Secure (3DS)	Product offered by card networks to enhance data elements from both the card issuer and the merchant to enhance security.

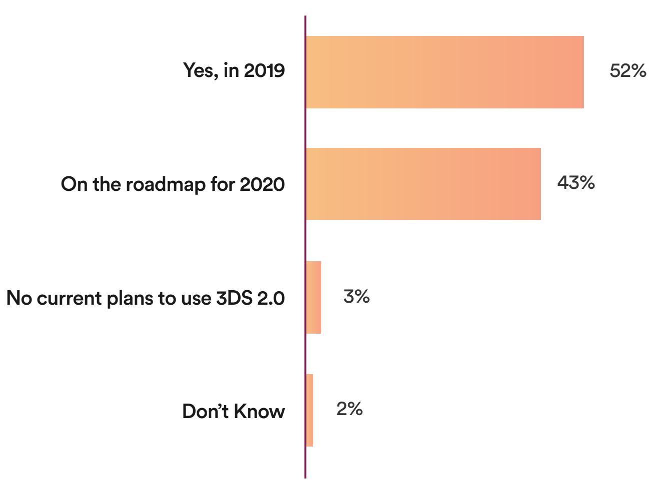
Q: Which automated fraud prevention solutions do you use?



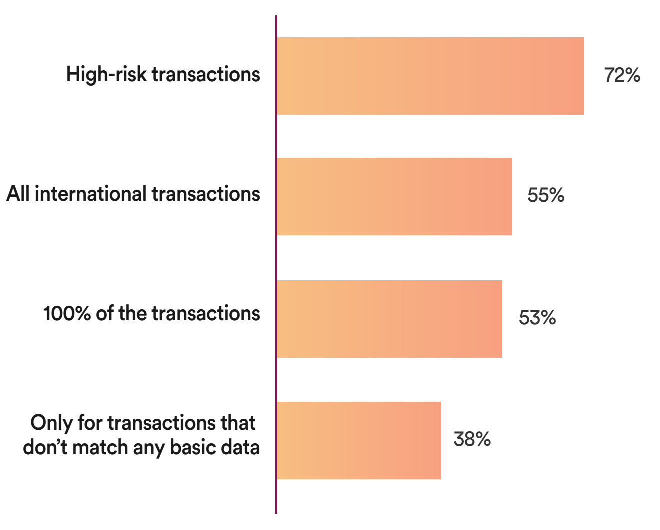
How Merchants Are Incorporating 3DS 2.0

3D Secure, also known as 3DS, is a payment network technology protocol that adds a layer of authentication to digital commerce transactions. With 3DS, the merchant sends additional contextual data about the transaction (such as device fingerprints, IP addresses, or shipping and billing addresses) to the issuer, which enables the issuer to better assess the transaction risk.

Q: Do you plan to deploy 3DS 2.0 in the next 18 months?



Q: For which transactions will you use 3DS 2.0?

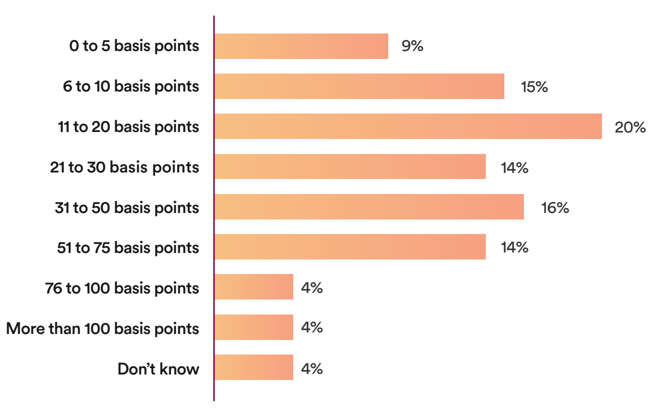


The Cost of Fraud Prevention

Fraud isn't cheap — and neither are the technology investments merchants must make to reduce fraud and protect the customer experience.

The merchants we surveyed are spending an increasingly large percentage of their revenue combating CNP fraud, with 30% spending between 0.21% and 0.5% of revenue in 2018.

Q: What did you spend on CNP fraud prevention as a % of revenue in 2018?

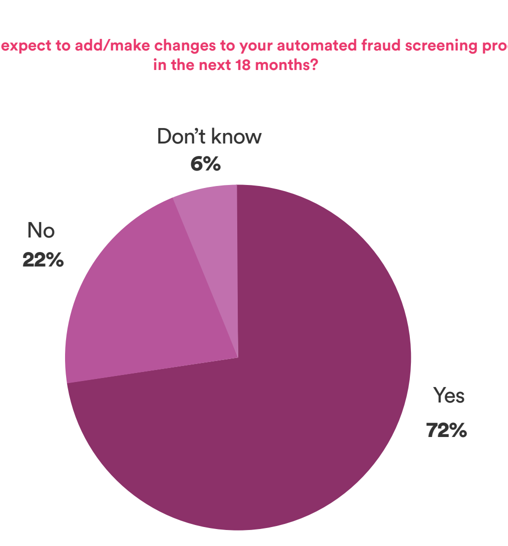


Making Changes in Fraud Prevention Strategies

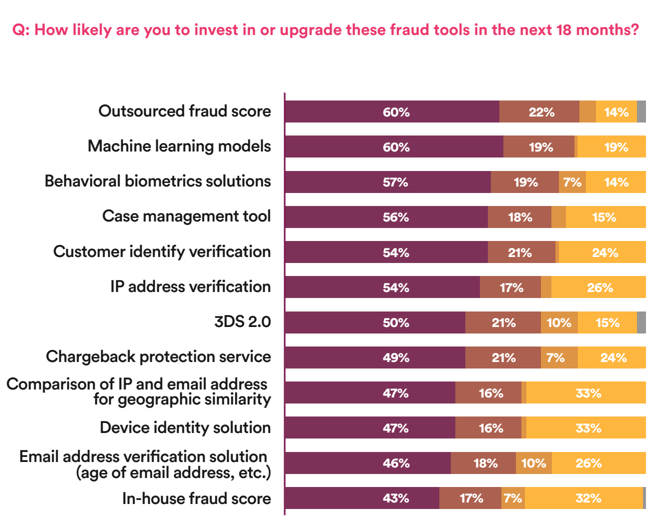
If merchants are learning anything in today's increasingly risky marketplace, it's that they need to take a flexible approach to fraud prevention. Just because they've invested in a solution doesn't mean it will always meet their needs, so it's important to be willing to consider new and more effective alternatives.

In fact, **72% of merchants surveyed are planning to add or make changes to their fraud solutions.**

Q: Do you expect to add/make changes to your automated fraud screening products in the next 18 months?



Q: How likely are you to invest in or upgrade these fraud tools in the next 18 months?



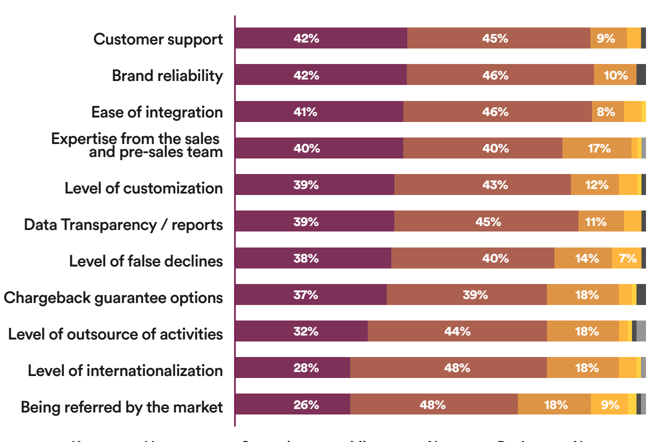
Choosing the Right Fraud Prevention Partner

While the factors listed above may convince an e-commerce merchant to implement fraud prevention measures, these factors alone don't explain how merchants choose their fraud prevention providers.

Many vendors offer all of these tools. How do merchants select a particular provider?

In our survey, 11 factors emerged as key influencers. The top three? Quality of customer service, the perceived reliability of the provider's brand, and the ease of integration.

Q: To what extent did each of these factors influence your selection of your current fraud prevention supplier?



ClearSale clients also appreciate high-quality customer service, as evidenced by our reviews.

"This is in line with our perceived feedback from our customers, who constantly recognize the importance of quality customer service." -- ClearSale client review on TrustPilot

See all Trustpilot reviews

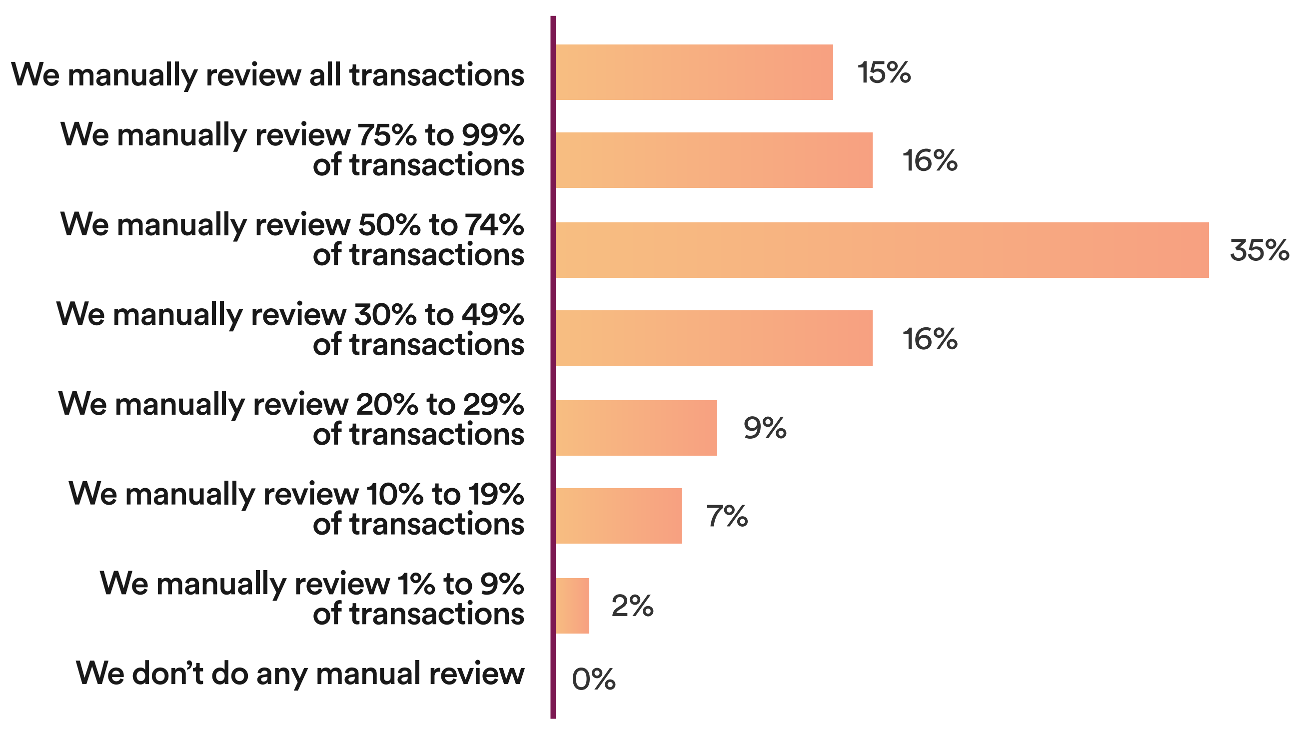
Manual Reviews and Automated Declines

Sometimes, correctly identifying fraudulent orders from good orders is like finding a needle in a haystack. The merchants we surveyed use multiple tactics to validate incoming orders, including both manually reviewing questionable orders and automatically declining highly suspicious orders.

The Prevalence of Manual Reviews

We were somewhat surprised to find that all our survey respondents review at least some of their transactions, and 15% review every transaction. Only 2% of merchants review fewer than 10% of transactions.

Q: What % of your sales transactions do you manually review?



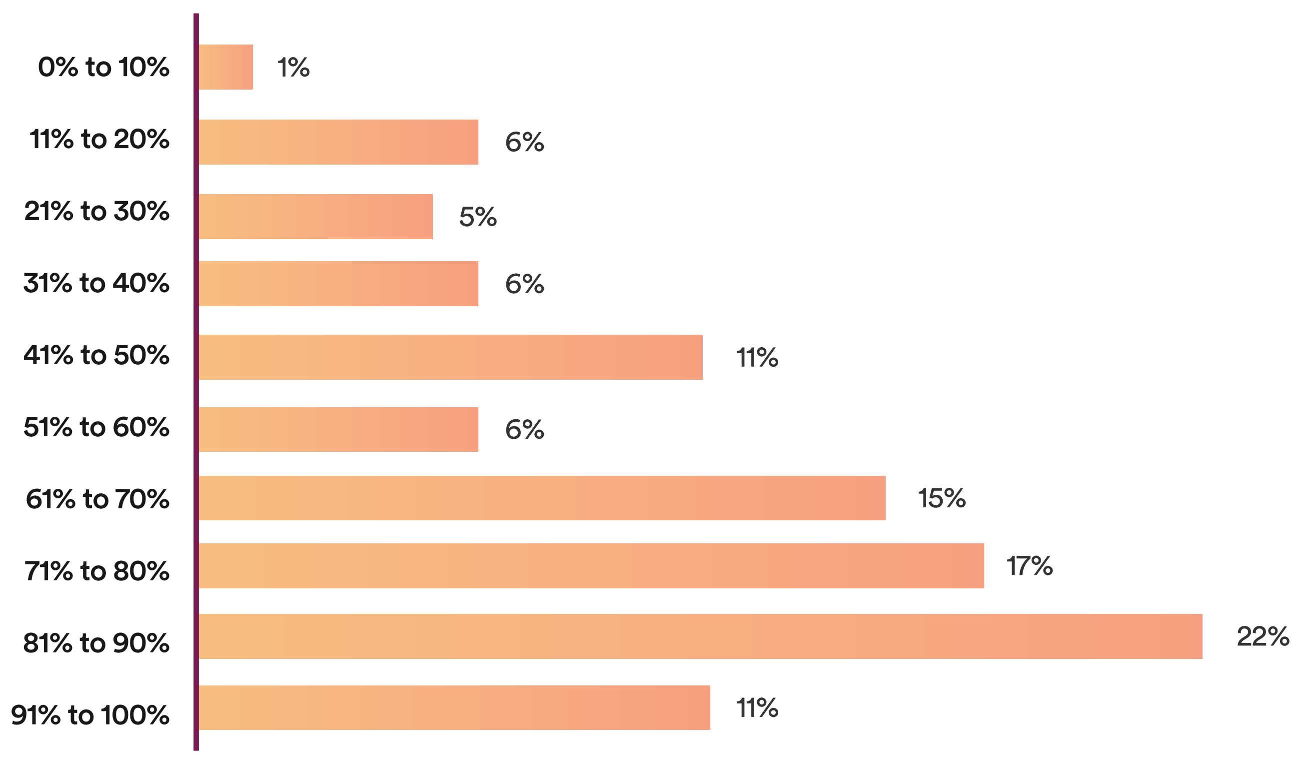
ClearSale's approach to fraud prevention means doing three things well:

1. Approve more good orders.
2. Stop more fraud.
3. Make decisions faster.

Our team of more than 700 specialized fraud analysts is the largest manual review team in the world and has been delivering the highest order approval rates since 2001.

Contact our sales team to learn more.

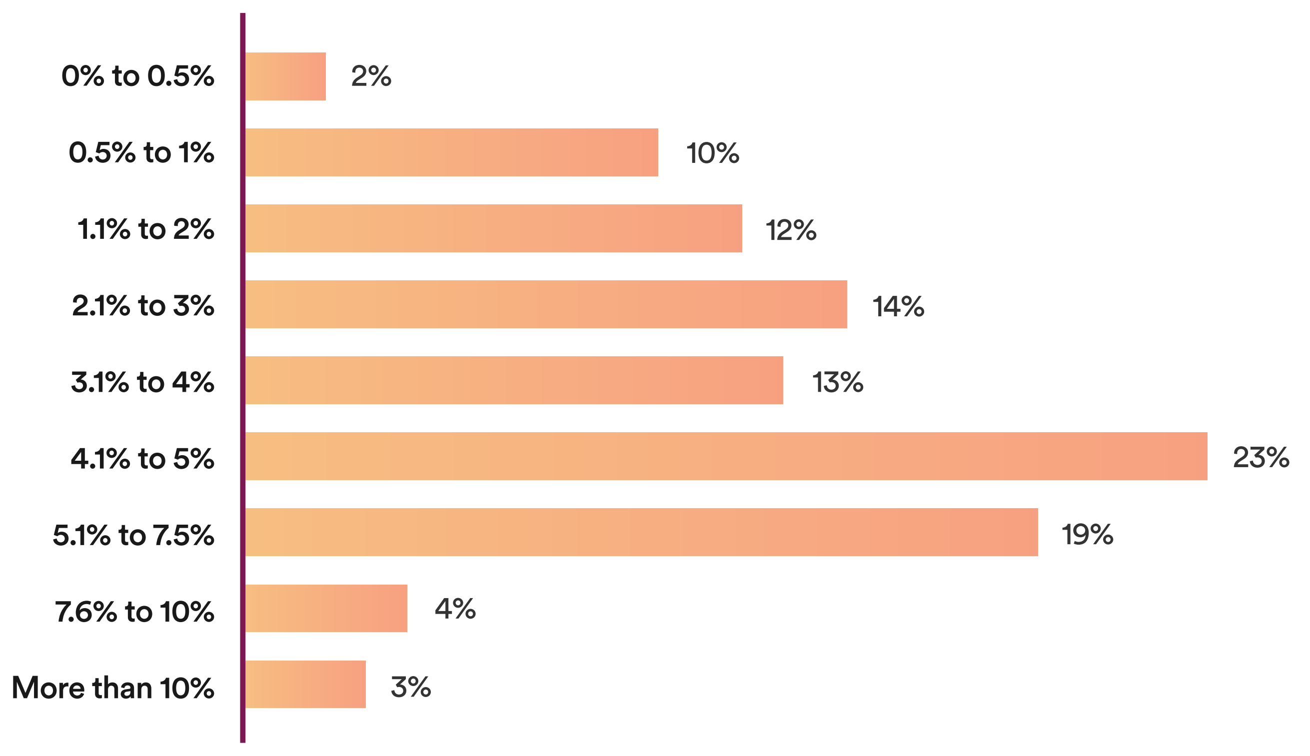
Q: What % of your sales transactions do you manually review?



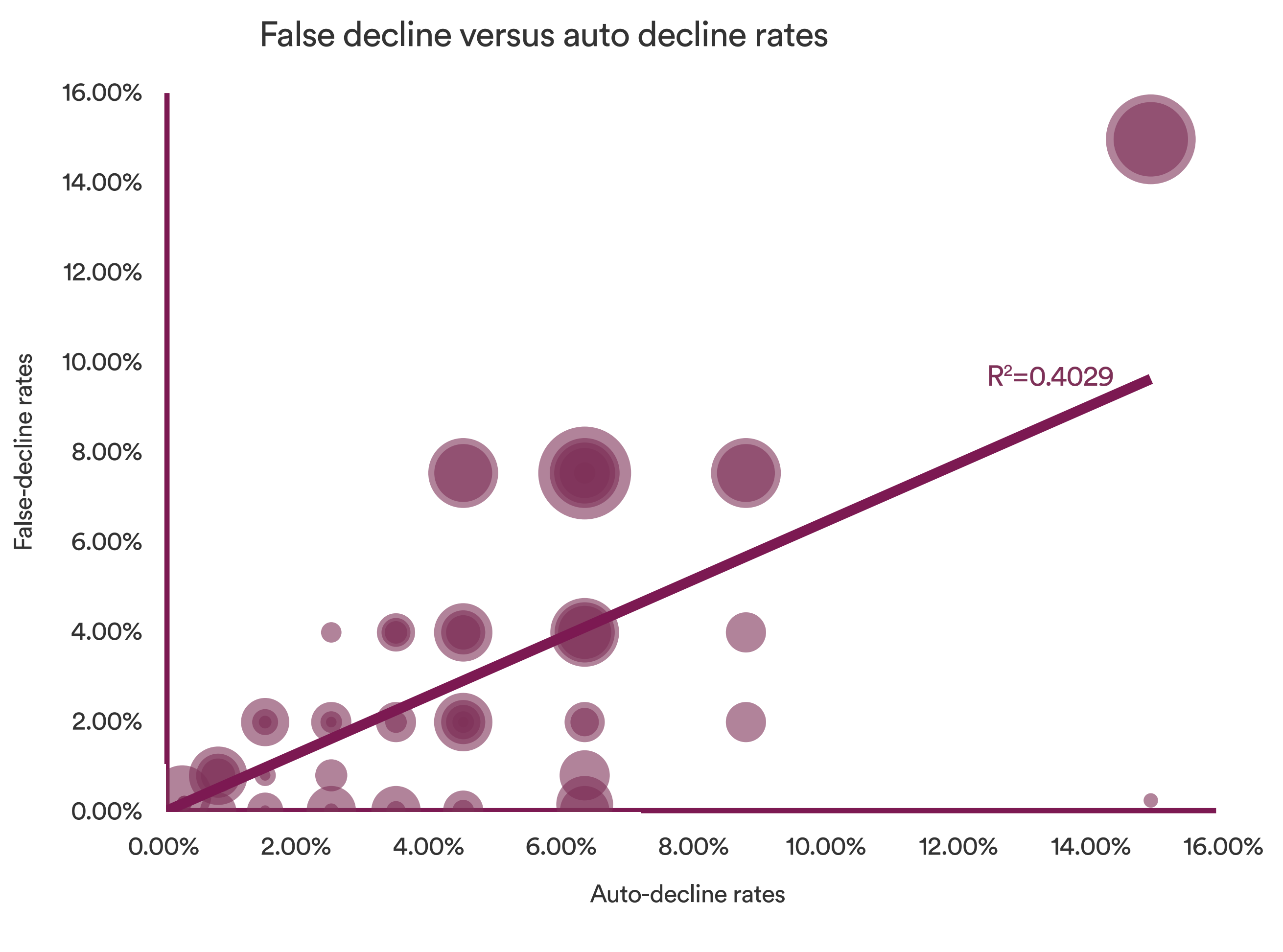
The Prevalence of Automated Declines

Given the inefficiencies around manual reviews, it may seem prudent to automatically decline orders that are highly suspicious. More than half of the merchants we surveyed report their fraud prevention solution automatically declines between 3.1% to 7.5% of all their transactions.

Q: What % of your sales transactions do you manually review?



In fact, there is a high correlation between auto-declines and false decline rates.



The Impact of False Declines

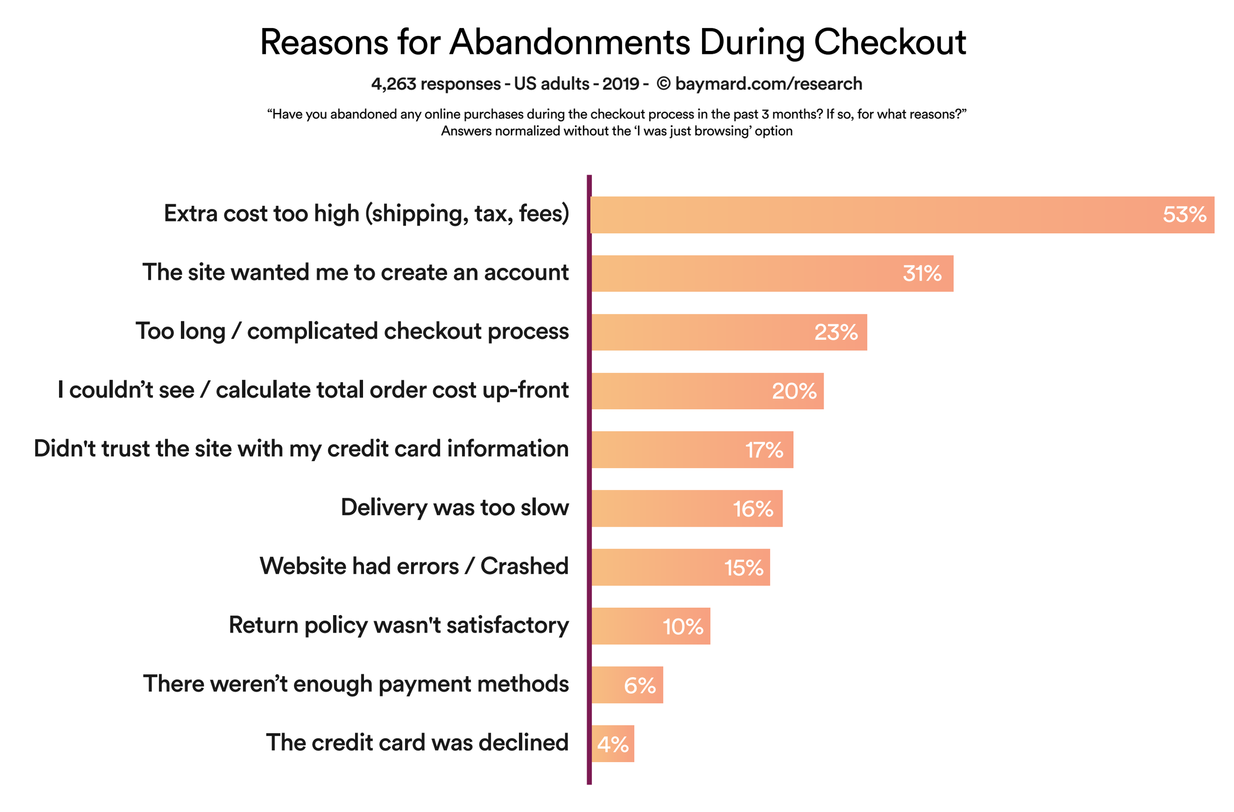
For both merchants and consumers, false declines are frustrating. False declines are good orders that end up declined due to suspicions of fraud – meaning the merchant loses a sale, and a customer is prevented from placing an order.

	Actual fraud	
Predict fraud	True positive	**Opportunity:** Revenue lost (false positive)
Predict legitimate	**Opportunity:** Chargebacks (false negative)	True negative

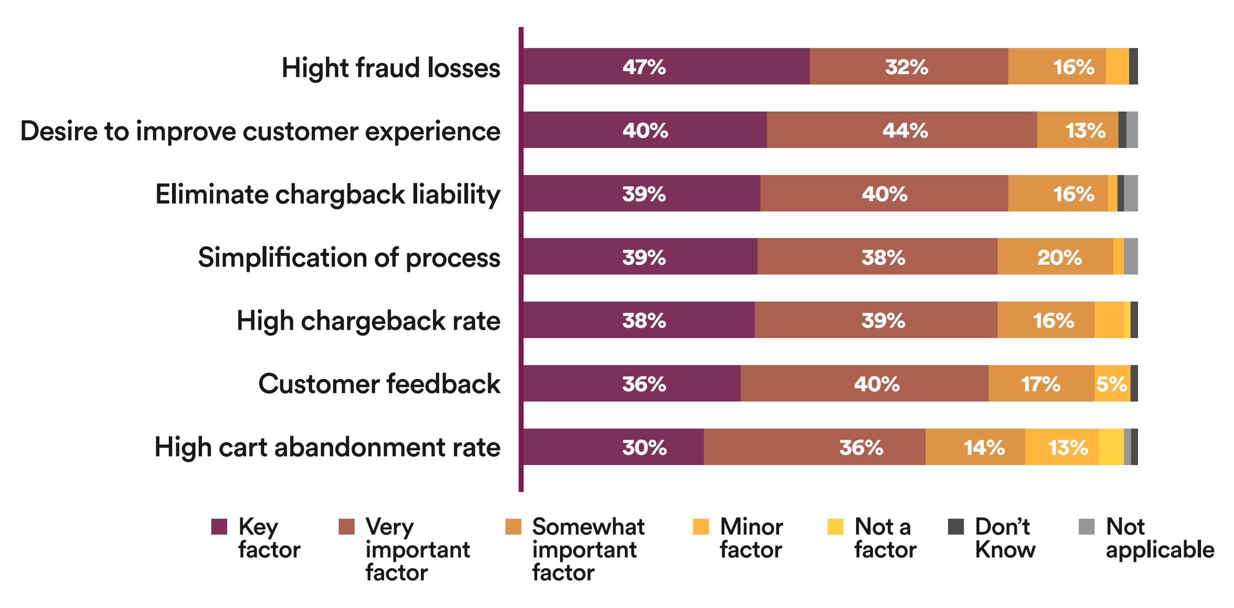
The Importance of the Customer Experience

The potential impact unhappy customers can have on revenue underscores just how important the customer experience is in online shopping:

- **A customer is 4x more likely to go to your competitor if a problem is service-related,** rather than price- or product-related. (Bain & Company)
- **Repeat customers spend 2x more** than new customers. (McKinsey)
- **96% of consumers classify customer service as an important factor** in their choice of loyalty to a brand. (Microsoft)
- **A promoter has a 1400% higher value** than a detractor. (Bain & Company)
- **Detractors are 2x as likely to talk** about bad brand experiences. (TARP Research)
- For every customer who complains to the customer support department, **there are 26 unhappy customers who don't bother to contact the company.** (TARP Research)



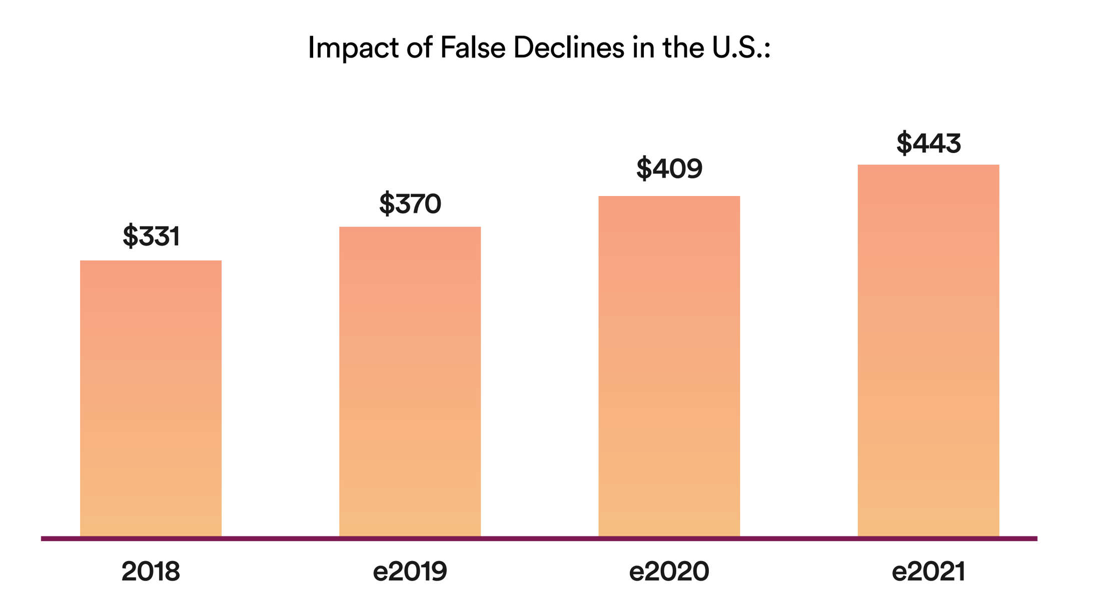
Q: To what extent did each of these factors lead to your decision to implement your current fraud prevention process?



Revenue Losses Due to False Declines

And here lies the issue with false declines: **E-commerce merchants need to prevent fraud – but if the fraud prevention process is too stringent or inflexible, the process will almost certainly incorrectly decline some percentage of good orders.**

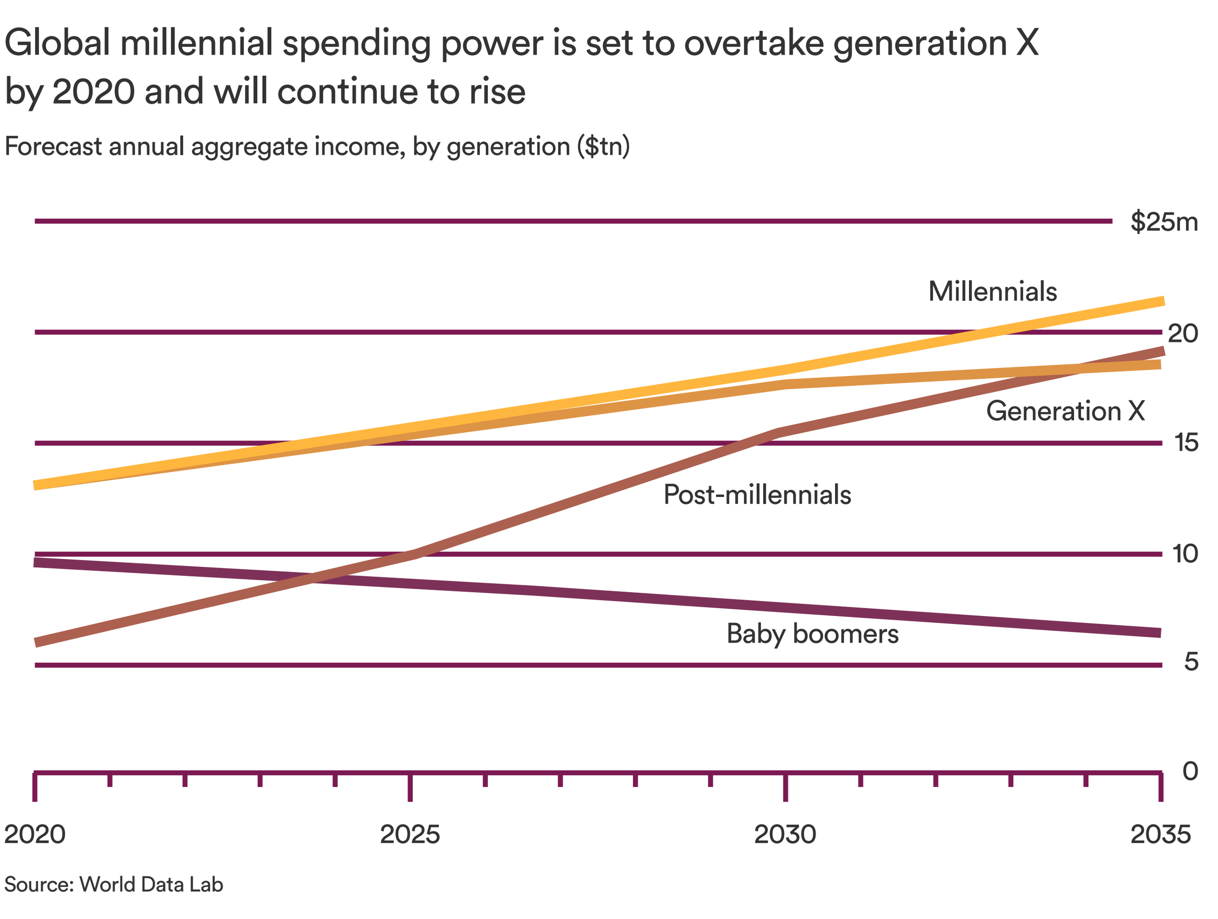
Just how high can these false declines get? Aite Group estimates that losses due to false declines will grow to $443 billion by 2021, up from $331 billion in 2018. Considering that e-commerce fraud only costs merchants $4.4 billion in 2018, this means **merchants lose 75x more revenue to false declines than they do to fraud.**



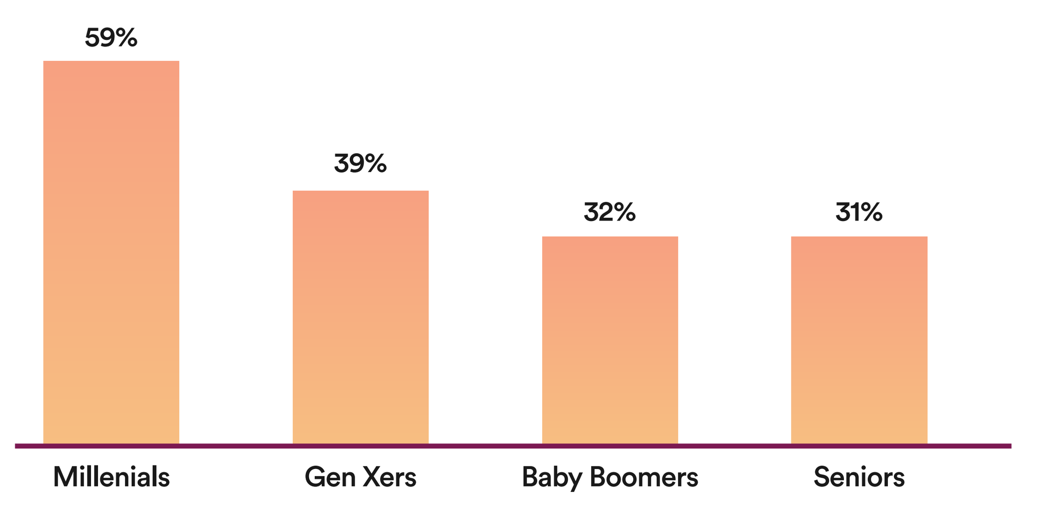
Generational Differences and False Declines

Another challenge with managing false declines is that different generations of consumers react to false declines differently.

Millennials – individuals who were born between 1981 and 1996 – make more than 50% of online purchases, and their spending power is growing, as demonstrated in the graph below. This is important for merchants, because Millennials have high expectations around their online shopping experiences. They are far less willing to forgive a merchant for a false decline than older generations might be.



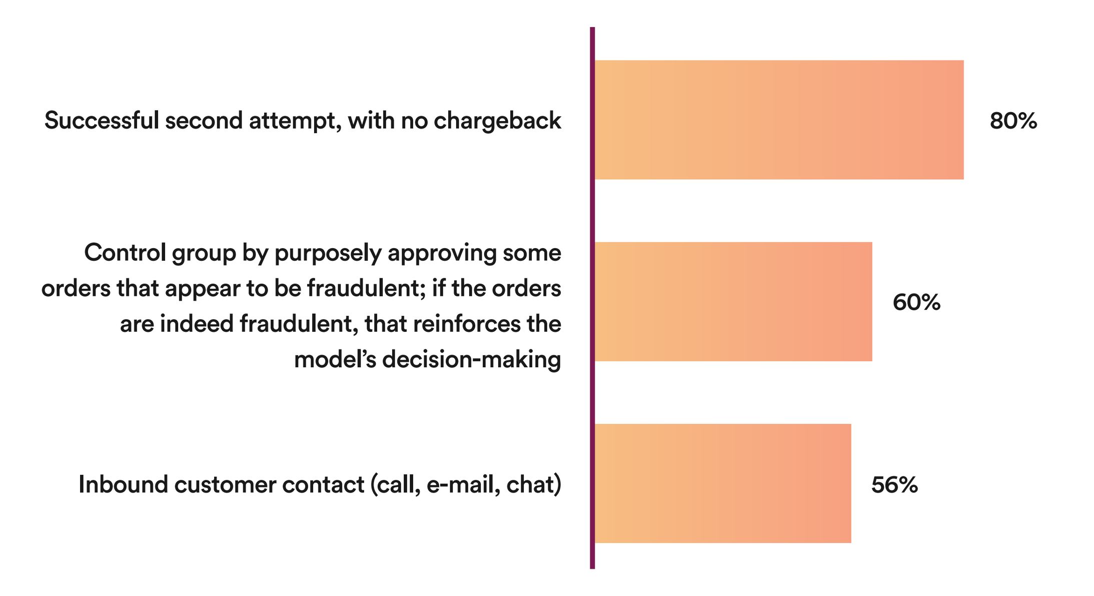
Q: Would you leave your financial institution due to a false decline?



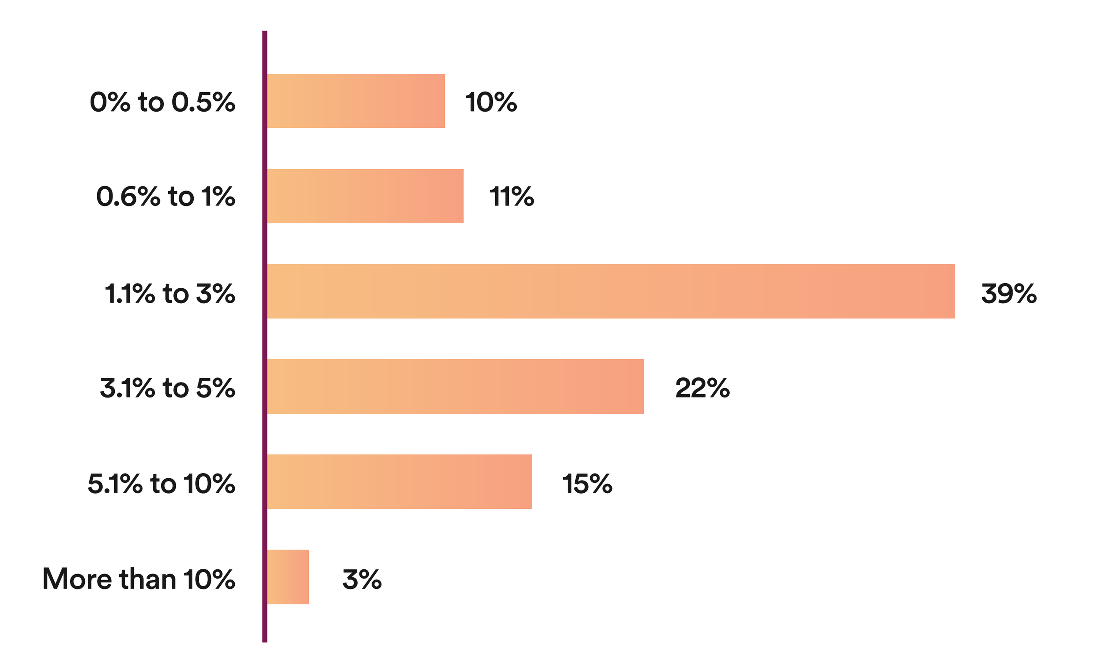
Measuring False Decline Rates

False declines are such a problem in the industry that 79% of merchants we surveyed measure false decline rates as a key metric.

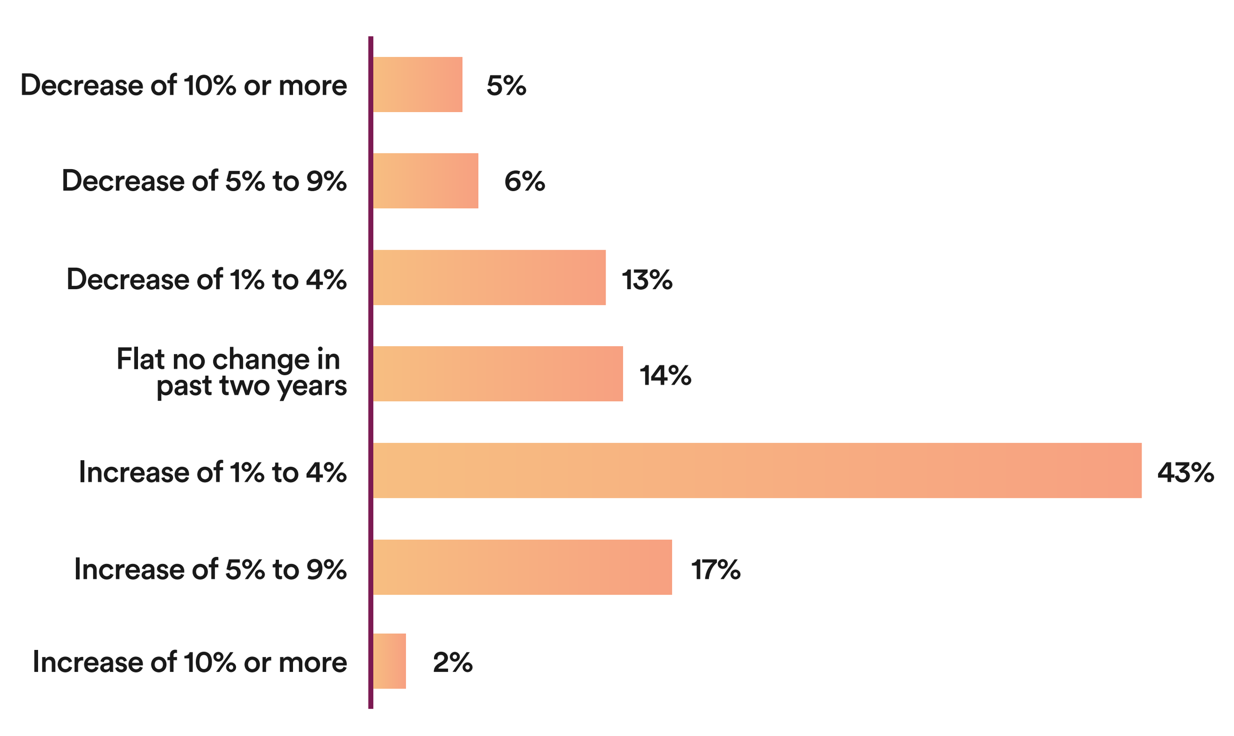
Q: How does your company identify false declines?



Q: What is your false decline rate?



Q: How much has your % of total declined transactions changed in the past two years?



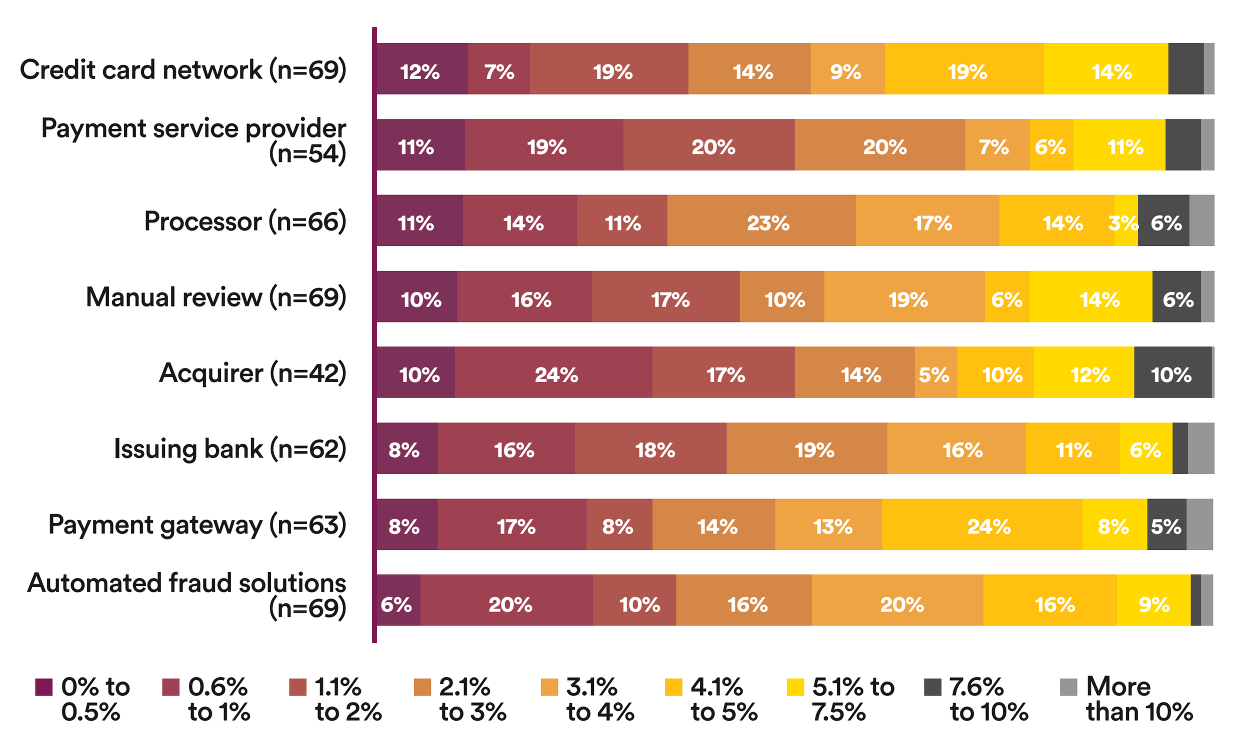
Understanding Where False Declines Happen

What makes reducing false declines even more challenging is that a transaction can be declined at any part of the authorization process — not just by the merchant, but by any party in the payment authorization process.

This is where measuring false declines can yield useful insights.

Our survey revealed that payment gateways and credit card networks are the most common sources of declines.

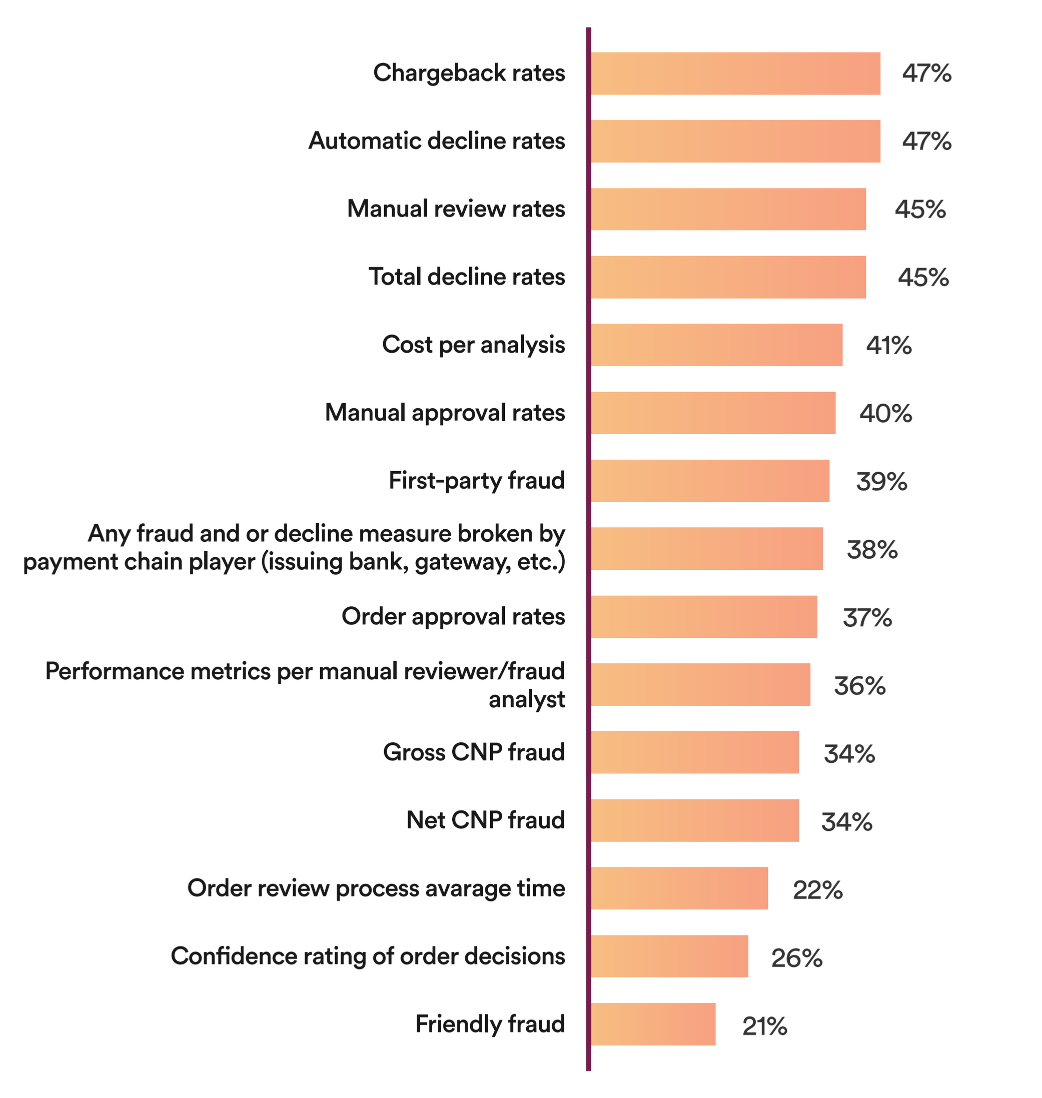
Q: How much has your % of total declined transactions changed in the past two years?



Other Important Fraud Metrics

When it comes to monitoring CNP fraud, the false decline rate is just one important metric to track. After all, if you can't measure it, you can't improve it. Here's what other key metrics merchants are keeping their eyes on when it comes to reducing fraud risk:

Q: What other key metrics related to CNP fraud do you measure?



Recommendations for Moving Forward

Tips for balancing false declines, fraud prevention, and the customer experience

While e-commerce fraud continues to escalate rapidly, false declines can also wreak havoc on revenue and customer relationships.

So, how can merchants balance fraud prevention, revenue, and the customer experience?

Here are four recommendations to consider implementing today:

- **Review current fraud prevention solutions.**
  Evaluate your CNP fraud protection and make sure it detects and prevents fraud without generating high false positive rates that can lead to costly manual reviews and potential false declines.

- **Communicate with the other parties in the payment approval chain.**
  Because a transaction can be falsely declined at any point in the payment approval process, talk with the other parties in your network to discuss how to work together to increase sales without increasing fraud losses.

- **Perform risk assessments.**
  Determine how and where fraud losses are occurring and whether additional fraud prevention layers can help mitigate those losses.

- **Understand the business case behind implementing a new fraud protection layer.**
  Whether you're thinking of adding a new fraud protection layer now or including it in future plans, your business case should consider any potential gains in operational efficiency and reduction in fraud losses. Also, consider that as other merchants implement more stringent fraud prevention strategies, organized crime rings will target less-protected merchants. Don't let that be you.

Our Data and Methodology

We conducted our research in May 2019 as a collaboration between ClearSale and Aite Group. Aite conducted an online survey of executives at 100 U.S. merchants with annual revenue between $100 million to $999.9 million.

To qualify for their survey, merchants with revenue between $100 million to $499 million had to generate at least 30% of their revenue via e-commerce, while merchants with revenue of $500 million to $999.9 million had to generate at least 20% of their revenue via e-commerce. Ultimately, 75% of the participating merchants generated at least 50% of their total annual sales via digital channels.

Q: What are the primary types of goods sold by your company?