EBOOK
APRIL 2025

The common good: Creating an ecosystem of transactional trust

How consumers, merchants, and issuers can move towards building an ecosystem of trust

Contents

Introduction

We're living in an ever-growing online world where everything from shopping to managing our finances is done online. While these experiences are convenient, they bring their own set of challenges.

Consumers expect online experiences that are both secure and seamless; strong enough to protect them from fraud yet effortless enough to avoid frustration. At the same time, organizations must strike a delicate balance: safeguarding transactions while maintaining trust and ensuring security measures don't disrupt the customer journey. Without it, consumers hesitate to shop online or entrust financial institutions with their money. And when businesses lose confidence in their customers, security measures tighten, adding friction to the experience. Striking the right balance between protection and seamless interactions is key to maintaining trust on both sides.

Building trust starts with secure data sharing. Consumers understand its importance and are willing to take extra steps to protect their transactions. For businesses, enhancing data-sharing practices will further strengthen security, creating a safer digital experience and reinforcing consumer confidence.

> *Our organization experience[s] online payment fraud, leading to financial losses, compromised customer trust and increased security measures.*
>
> **Board member of an e-commerce organization**

Throughout this report, we refer to:

- **Consumers:** Those who have used a mobile app or a website to buy something online or to manage their finances in the last month
- **Merchants:** Any organization who sells their own products or where consumers can buy from third party sellers
- **Issuers:** Online banking or financial services organizations

Creating this "ecosystem of trust" between all three parties is fundamental to ensure there is a frictionless transaction experience for consumers and merchants and issuers. To better understand this dynamic, research was undertaken to explore the relationship between consumers, merchants and issuers in online interactions.

This report aims to complement the groundwork and findings laid out in our 2023 report with the growing emphasis on trust and the need for frictionless experiences. The 2024 report is focused on identifying the foundations of trust, how fraud can lead to an erosion of trust and how all parties can move towards building this ecosystem of trust. To give a balanced view, this report examines the dynamics of trust through the lens of all three parties — consumers and the organizations that they interact with online, that is the issuers and the merchants.

Key findings

Navigating towards an ecosystem of trust

A balanced approach with strong security, seamless experiences and responsible data sharing is key to building trust in digital transactions.

Security is the top priority for consumers, but excessive friction in transactions can undermine their trust.

- 77% of consumers **prioritize security over speed** when shopping online, 79% in case of financial transactions. However, overly sensitive fraud prevention can trigger frustration.
- More than half of merchants (56%) and nearly half of issuers (49%) **are improving payment processes, focusing on security while ensuring a smoother customer experience.**

Data sharing strengthens fraud prevention.

- 77% of consumers **would share more data when shopping online** while 76% would do so with financial institutions, to help combat fraud.
- Issuers (63%) are more likely than merchants (30%) to share additional data for all transactions to improve fraud detection.

The foundation of trust

Consumers remain cautious about sharing personal data, making trust a critical factor in digital transactions.

- Despite the willingness, 83% of consumers still have concerns sharing their personal data with mobile apps or websites, and **49% say trust in online stores is "absolutely crucial."** Although fewer (76%) have data-sharing concerns with online banks, **trust remains "absolutely crucial"** for 67% of consumers.

Fraud concerns vary between **merchants and issuers.**

- 39% of merchants worry about being classified as high risk from fraud, leading to increased transaction fees. Top concerns among issuers are emerging (35%) and increasingly sophisticated (34%) fraud tactics.

Fraud and the erosion of trust

Fraud damages both consumer confidence and business reputation.

- 92% of consumers **would trust a company less**, while 91% would consider not using that company altogether, if they experienced fraud whilst making a purchase.
- To tackle fraud, whether targeting consumers or originating from them, such as first-party fraud, virtually all organizations are taking proactive measures to strengthen security and protect trust.

All statements made above are derived from Mastercard-commissioned Vanson Bourne research.

Section 1: Navigating towards an ecosystem of trust

Ecosystem of Trust: A secure digital environment where consumers, merchants, and issuers cooperatively share data and collaborate to reduce fraud.

Transactional trust is not a one-way street; it's a complex interplay between consumers, merchants and issuers. In other words, it's an ecosystem of trust. Each party has their own needs within this relationship, and a shared commitment is vital to ensuring these needs are met for all. One way to build trust is by collaborating in a meaningful data exchange to heighten the accuracy of detecting fraudulent behavior.

"Fraudsters used customer information to manipulate customer accounts, causing damage to customer interests and reducing customer trust in us. We will improve the security of our system and set up more verification to ensure customer safety.

Board member of a retail organization

While it is essential for consumers to trust the banks or the organizations from which they purchase, especially when sharing personal data, they are still willing to take extra measures to create a more secure experience. Overall, 68% of consumers would be willing to share more personal data when making purchases online, while 71% of consumers are willing to share more online spending data with financial institutions. Consumer openness is driven by a clear purpose: strengthening fraud prevention and ensuring a safer digital experience for everyone.

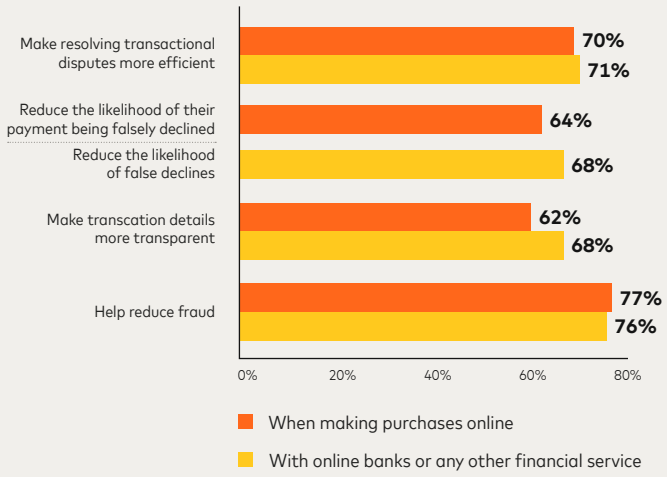


Figure one shows where consumers more and least willing to share personal data when making online purchases, or with online banks or any other financial services

This willingness to share data to help reduce fraud also extends to merchants and issuers. Most merchants and issuers currently share data beyond what is mandatory for some or all transactions with the other party. However, while 63% of issuers share data beyond what is mandatory for all transactions, only 30% of merchants do this.

"Our organization plans to work closely with payment processors, banks and regulatory bodies to share information, detect emerging threats and implement best practices for fraud prevention across the industry.

Board member of a crypto-banking organization

With the clear benefits of data sharing for compliance and regulatory strength, merchants must close the gap and embrace a more collaborative approach.

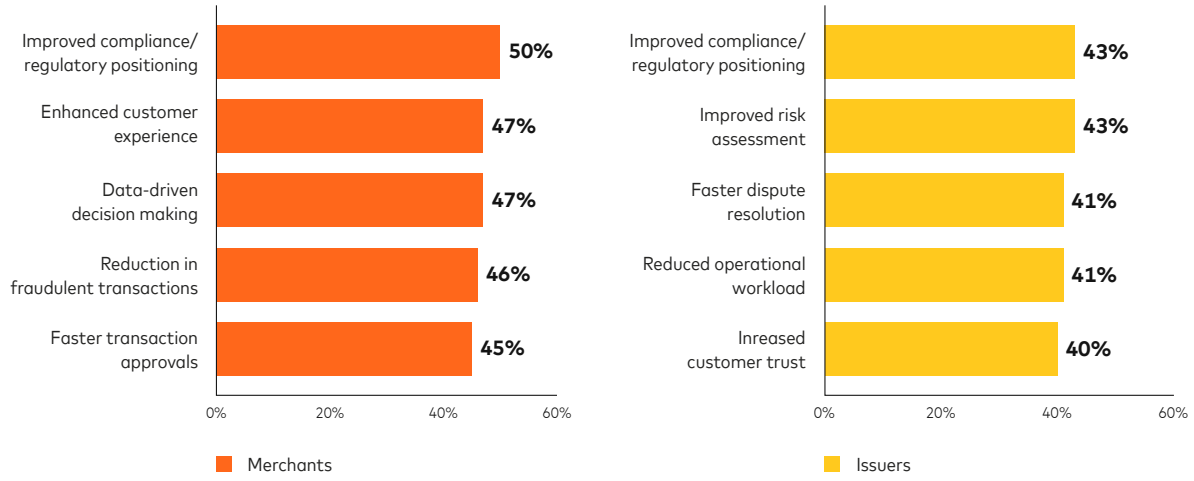


Figure two showing what operational improvements organizations have seen from sharing data with issuers/ merchants to verify digital identities of their customers.

For those merchants sharing this additional data for **all** transactions, almost half (46%) have seen revenue protection/ growth benefits, compared to less than 4 in 10 (37%) for those only sharing data for **some** transactions.

Combatting fraud

For organizations, strengthening fraud prevention isn't just about sharing data externally, it's also about building trust from the inside out. By proactively integrating fraud prevention solutions, businesses safeguard revenue while reinforcing consumer confidence and trust. The positive consequence of this could lead to reduced customer churn and reputational improvements. Virtually all merchants and issuers in this research have taken steps to reduce online payment fraud. The most common approach by merchants is to deploy customer identity verification (62%) and use multi-factor authentication to secure accounts (also 62%). For issuers, customer identify verification is the most taken step (50%). From the steps organizations have taken to reduce online payment fraud, customer identity verification has been the most effective at tackling this type of fraud.

> *My organization's approach now emphasizes proactive measures, such as regular audits and AI-powered fraud detection, to enhance payment security.*
>
> **Board member of a FinTech organization**

Despite efforts to reduce fraud, almost 6 in 10 (57%) consumers in this research were still very or extremely concerned their identity would be stolen or they'd become a victim of fraud at some point in the future, increasing slightly since 2023 (55%). This could be because the amount of fraud experienced by consumers when transacting online hasn't reduced in the same time frame (2023: 28% - 2024: 29%). This suggests that despite the steps organizations are currently taking to reduce fraud, this has not trickled down to consumers, who are still burdened with the same levels of fraud as 18 months ago. As public awareness of scams and data breaches is becoming more widespread, this could also contribute to why high levels of concern remain.

The risk of experience decay

Although 77% of consumers say they would prefer a secure over speedy online purchase experience, and 79% say the same about using online financial services, organizations need to be wary of 'experience decay'. In the pursuit of greater security, if consumers must repeatedly re-authenticate or re-enter their information, it may lead them to abandon their purchase or stop using the service altogether. For example, 85% of consumers would give their email address when creating an account to make a purchase online, but only 43% would re-enter the same information when completing a transaction. In fact, almost 1 in 3 (28%) consumers have abandoned a transaction online after becoming impatient with the length of time it took to enter their details.

An important point to remember is that consumers are not 'one-size-fits-all'. Some consumers want a rapid and convenient transaction experience, whilst others (77%) are more security conscious. Gen Z consumers are almost 2.5 times more likely to state they want a speedy online purchase journey compared to Baby Boomers.

In this report, consumers are categorized into their generational age groups.

- **Gen Z:** 18-27 years old
- **Millennials:** 28-43 years old
- **Gen X:** 44-59 years old
- **Baby Boomers:** 60+ years old

Only those 18 and over were surveyed. Correct at the time of data collection – 2024

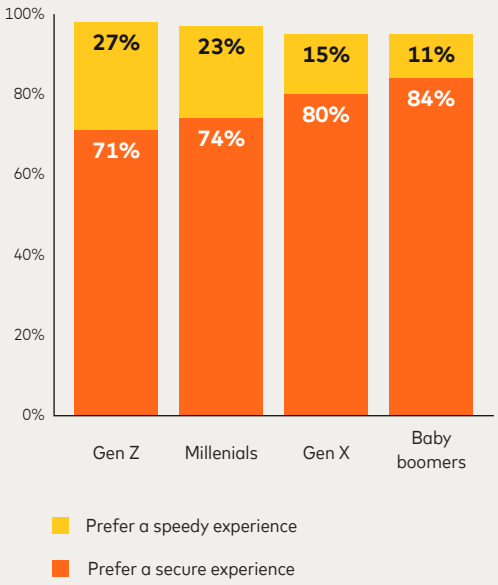


Figure three shows when making a purchase online, would consumers prefer an experience which was speedy/ convenient (but less secure) or secure (but less speedy/ convenient).

The most effective way of balancing security and convenience with consumers is by optimizing payment handling and processing. Over half of merchants (56%), and just under half of issuers (49%) are currently undertaking steps towards this optimization. Merchants are most likely to be currently undertaking checkout process simplification (60%), and issuers are introducing a greater variety of payment options (53%).

In pursuing this optimization, organizations are continuing to factor in security. Integrating secure, real-time data verification to reduce the need for customers to re-enter information is the primary step being taken by both merchants (59%) and issuers (48%). In addition, implementing seamless authentication methods that secure transactions without adding complexity is the second most undertaken step by merchants (57%), and third for issuers (44%).

Building a trusted transaction ecosystem requires collaboration between consumers, merchants, and issuers to stay ahead of fraud. Consumers are open to sharing more data for enhanced security, yet merchants have yet to fully embrace the benefits of data-sharing like issuers have. The challenge lies in balance, security must be strong but not obstructive. If measures are too complex, customers may walk away. But when done right, organizations not only prevent fraud, but they also cultivate trust, fuel growth, and deepen customer relationships.

All statements made above are derived from Mastercard-commissioned Vanson Bourne research.

Section 2:
The foundations of trust

Today's consumers have the digital world at their fingertips, doing everything from ordering groceries to banking solely online. This has made our lives significantly easier but also led to a frontier of new challenges and concerns. From the consumer side, it's how to stay safe online, and for organizations it's how to ensure fraud does not eat away at their bottom line.

A key underpinning of these concerns is trust. Consumers will only transact with trusted sources. While organizations need to have tools in place to ensure consumers interacting with them are who they say they are.

From the consumers' side, personal data is a key worry. 83% of consumers have concerns about their data when making a purchase online and 76% have concerns when sharing information with online financial institutions. The main concerns are centered around the fear of their data being stolen and falling victim to fraud. Unsurprisingly therefore, around half (49%) of consumers say it's absolutely crucial to have trust in an online store when sharing personal data, and almost 7/10 (67%) say trust is absolutely crucial when sharing data with a bank or other online financial institution. And this need for trust is only growing. In research we conducted in 2023, 40% of consumers said it's absolutely crucial they trust an online store when making a purchase and 65% said the same about the use of online financial institutions.

VOICE OF THE CONSUMER

Meet Nicola*

Nicola is highly tech savvy and takes her online security very seriously. She only shops at and uses platforms she trusts. Her trust is hard to build, but easy to lose. Despite strong concerns around security, she is not overwhelmingly willing to share more data with merchants or online financial institutions, even if it helps reduce fraud.

For the Nicolas's of the world...
61% are Gen X or Millennials, 55% are women

In response to their bank challenging and legitimately declining a transaction

"I forgot to alert my bank that I was traveling. It made me feel relieved because it proved to me that my bank has legitimate security measures in place to protect myself and my account".

34%

have been the victim of fraud within the last three years

68%

would be willing to share more personal data with merchants to make resolving transactional disputes more efficient

78%

would be willing to share more personal data with merchants to help reduce fraud

82%

would prefer a secure over speedy experience when making an online purchase

98%

would not use a company again if they experienced fraudulent activity when making an online purchase

*Personas have been created from aggregating respondents with shared characteristics [n=331]. This persona does not represent an actual person.

VOICE OF THE CONSUMER

Meet Jason*

Jason likes to make weekly online purchases for groceries, as well as clothing. Typically, he spends around $200 online a week. When making purchases, convenience is key, and he prefers experiences which are speedy over secure. Despite his regular online spending, he has never been a victim of fraud.

For the Jason's of the world...
72% are Gen Z or Millennials, 53% are men

In response to having a transaction falsely declined

"Just made me worry about the validity of my card, and then wonder about how well their site must be run."

88%

have concerns about their personal data when making **purchases online**

43%

feel it's **absolutely crucial** they trust the merchant they're making an online purchase with when sharing personal data

97%

would be willing to share more personal data with merchants to help reduce fraud

70%

are very or extremely concerned that they'll become a victim of fraud or identity theft in the future

90%

would trust a merchant less in the future if they experienced fraudulent activities when using the platform

*Personas have been created from aggregating respondents with shared characteristics [n=60]. This persona does not represent an actual person.

Fraud remains a major challenge for organizations, demanding constant vigilance and strategic action. For merchants, it's a concern that financial institutions will deem them at high risk of fraud, leading to them experiencing higher transaction fees (39%). The emergence of new (35%) and ever more sophisticated fraud tactics (34%) are among the top concerns for issuers. This had led to both merchants and issuers unanimously taking steps to reduce the risk of online payment fraud.

In pivoting towards a security-first approach, organizations need to be conscious of the impact of additional security challenges and processes. For example, false transaction declines caused by certain security protocols can have a negative effect on consumer trust.

"It [false transaction decline] made me confused and also a little anxious. Yes, it did change my behavior and the declined transaction made me trust the company less after that. The declined transaction also affected my trust in the payment process, as I didn't think that it was safe."

Generation Z (18-27 years old)

Fraud presents challenges, but organizations that prioritize security and trust can turn risk into opportunity. A strong fraud prevention strategy not only protects customers but also strengthens brand reputation and customer loyalty. When consumers feel safe, they are more likely to return, advocate for the brand, and build lasting relationships, turning trust into a competitive advantage.

VOICE OF THE CONSUMER

Meet Patricia*

Although not a regular spender online, she is a prolific checker of her online banking and investment apps. But when she does make online purchases, she has concerns about her personal data.

For the Patrcia's of the world...
68% are Gen X or Baby Boomers, 51% are woman

In response to having a transaction falsely declined

"It is irritating and I have changed my mind about using the site. I have also called my credit card provider to find out why"

65%	72%	74%	79%	52%
have concerns about sharing their personal data with issuers in case it is stolen and they fall victim to fraud	feel it's **absolutely crucial** they trust the issuers they're sharing personal data with	**would be willing** to share more online spending data with issuers if it helps to reduce fraud	**would prefer a secure over speedy** experience when using an online bank or other financial service	would be extremely likely to **not use a company again** if they experienced fraudulent activity when making an online purchase

*Personas have been created from aggregating respondents with shared characteristics [n=307]. This persona does not represent an actual person.

Section 3: Fraud and the erosion of trust

Given that fraud can impact both organizations and consumers, how does this lead to a breakdown in trust, and what positive measures are both parties taking in response?

How likely is it that you would do the following if you were to experience fraudulent activity when using a company's mobile app or website?

Churn

91%

would not use that company again in the future

Trust

92%

would trust that company less in the future

Reputational damage

92%

would complain to the company directly

65%

would post negative feedback online about the company

89%

would tell other consumers/ users about the fraudulent activity

Fraud isn't just something consumers experience, it's also something they can commit, whether intentionally or not. This delicate balance of trust creates friction; relying too heavily on consumer integrity can leave organizations vulnerable to significant risk. One type of such fraud is first-party fraud, or friendly fraud which is defined as consumers erroneously disputing a transaction.

We estimate that first-party fraud costs organizations approximately $50bn per year. Complexity arises because first-party fraud can be accidental, usually caused by unclear merchant information leading to a query about the transaction, or maliciously, such as through fraudsters initiating chargebacks.

An ecosystem of trust in the wild: Fighting back against first-party fraud

With current global ecommerce levels on the rise, increased safety and transparency of payments for merchants and issuers is a necessity. Our First-Party Trust program, with AI-powered insights, was developed with industry groups including US Merchant Advisory Group and Merchant Risk Council to combat the surging trend in 'friendly' fraud, where genuine transactions are mistakenly or intentionally challenged by consumers/ cardholders.

The First-Party Trust program addresses first-party or friendly-fraud by bridging the gap between parties to enable better data sharing. Merchants and issuers will now be equipped with the tools and technology to prove genuine purchases and prevent flawed disputes. And consumers can better recognize transactions on online statements and enjoy seamless, secure, and frictionless experience.

To learn more, visit
https://b2b.mastercard.com/first-party-trust

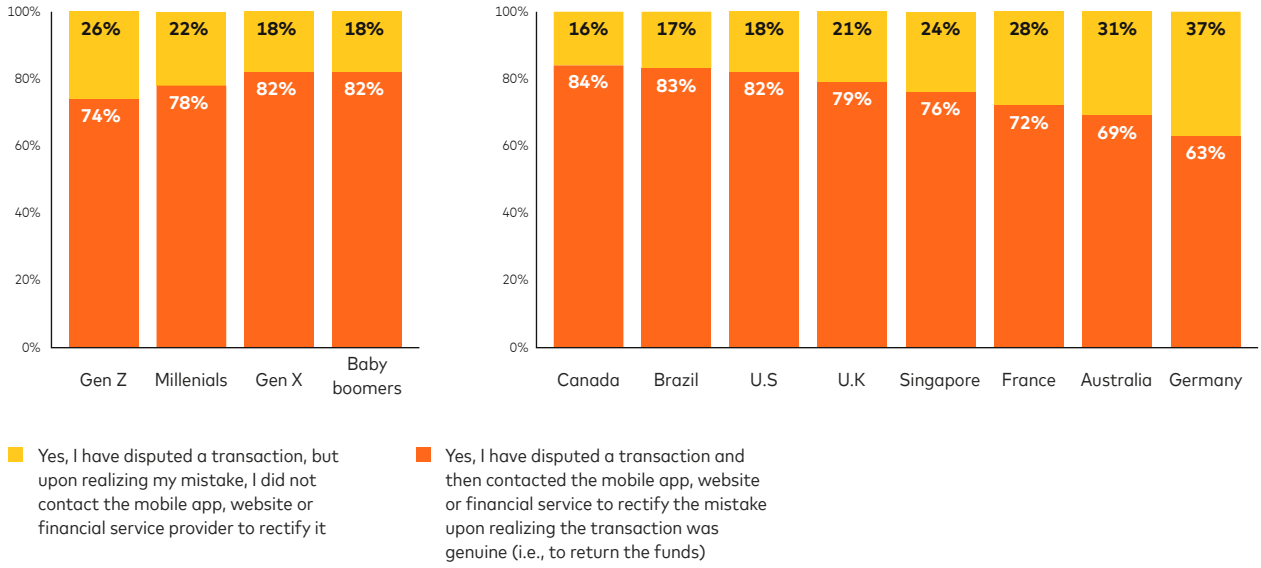
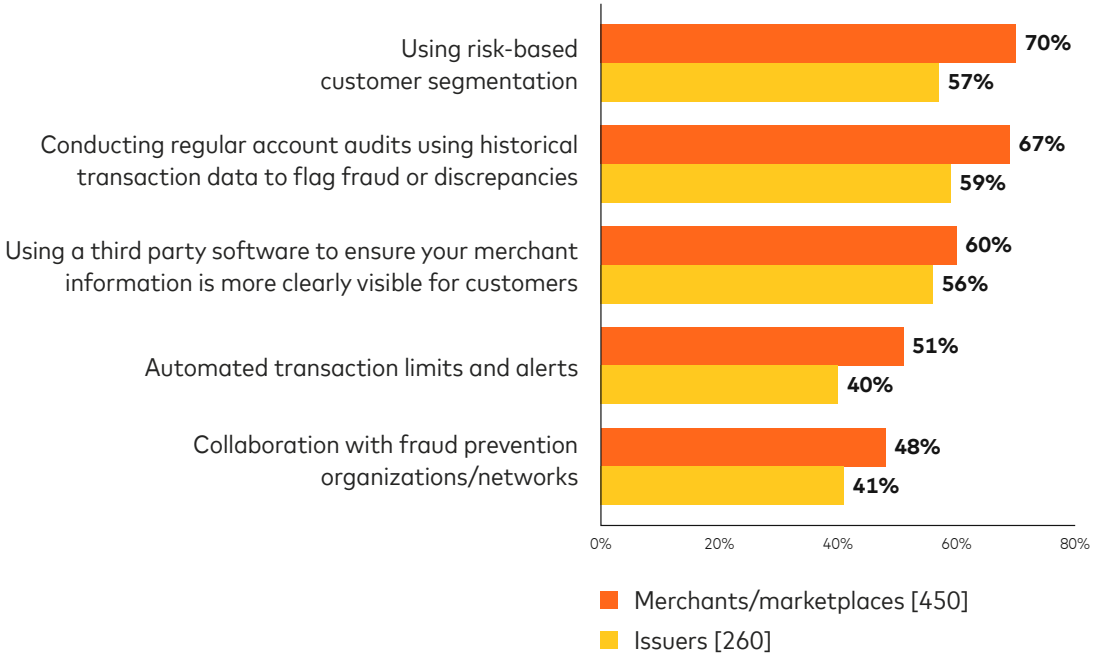


Figure four shows where consumers have disputed a transaction and realized it was a genuine mistake, what they then proceeded to do. Out of the 4,500 consumers that were surveyed, 775 had disputed a transaction.

For the most part, consumers take an honest approach. For the 34% of consumers in this research that did make a transaction dispute erroneously, almost 78% contacted the organization to rectify the mistake. However, 22% of those consumers that did dispute a transaction did not rectify the erroneous refund even after they realized their mistake, in other words, they committed first-party fraud. Despite the overwhelming honest approach from consumers, there is some nuance here, with younger consumers and those in Germany, being the least likely relatively to take action to rectify their mistake.

First-party fraud takes many forms, underpinning why organizations take a multitude of actions to try and combat it. For merchants, their top course of action is to use risk-based customer segmentation, performing additional checks on consumers they've deemed higher risk (70%). For issuers, their top approach is to conduct regular audits, using historical transaction data to flag potential fraud or discrepancies (59%).



It's not only first-party fraud that organizations must be wary of. Other types of online payment fraud also have significant impacts. It is predicted that the cumulative losses to merchants from online payment fraud globally between now and 2027 will exceed $343 billion. This fraud will not only impact merchants, but issuers as well through increases in reimbursements to cardholders for example. Consumers will also be impacted through inflated costs of goods or increased authentication challenges. Issuers are increasingly looking to fight fire with fire, integrating more sophisticated technology, such as AI, to outcompete with emerging and complicated threats.

> *Real-time fraud detection powered by AI is the area where our organization is focusing when looking to combat online payment fraud in the future.*
>
> **Board member of a banking organization**

Fraud is complex, but at its core, it's a trust issue. For consumers, fraud shakes confidence in an organization's ability to protect their purchases and financial security. For businesses, trust is tested in two ways: can they be sure consumers are who they claim to be? And can they trust consumers to be honest about their transactions?

Conclusion and methodology

Conclusion

Trust is the cornerstone of the digital transaction economy. It is an essential element that binds consumers, merchants, and issuers. This research highlights the delicate balance these groups must strike to build a system that is resilient, secure and frictionless.

Consumers are willing to share more data to combat fraud, but this trust comes with a clear expectation: organizations must safeguard their information while delivering a smooth, secure experience. While issuers have embraced data-sharing to strengthen their defenses, merchants have yet to fully capitalize on its potential. Closing this gap is critical, not only to reduce fraud but also to unlock tangible benefits, such as improved revenue protection and growth for merchants and issuers.

Organizations must navigate the dual challenge of enhancing security without alienating customers through overly complex transactional processes. Consumers are not a monolith; their needs differ across demographics, with some prioritizing speed and others valuing security above all else. Striking the right balance is vital. Streamlined authentication methods and real-time data verification offer pathways to meet these diverse expectations while maintaining trust.

Fraud remains a persistent and evolving threat. Its impact extends far beyond financial losses, eroding the trust that underpins consumer relationships and organizational reputation. From first-party fraud to sophisticated cyberattacks, the message is clear: combating fraud requires vigilance, collaboration, and innovation.

By making trust the priority, through innovation, shared intelligence, and seamless security, organizations don't just mitigate risk. They create a stronger, safer, and more resilient digital economy, where trust is not only restored but reinforced.

Methodology

Mastercard commissioned independent market research agency Vanson Bourne to conduct 5,210 quantitative interviews in total across three audiences:

- Consumers who had used either a marketplace, merchant and/or online bank/other online financial service within the past month: 4,500 interviews
- Decision-makers in merchants and marketplace organizations: 450 interviews
- Decision-makers in financial services belonging to organizations such as banks and crypto exchanges: 260 interviews

The research was conducted between November and December 2024 across a number of different countries including US, Canada, UK, Germany, France, Australia, Singapore and Brazil.

All interviews were conducted using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

About us

About Mastercard

Mastercard powers economies and empowers people in 200+ countries and territories worldwide. Together with our customers, we're building a sustainable economy where everyone can prosper. We support a wide range of digital payments choices, making transactions secure, simple, smart and accessible. Our technology and innovation, partnerships and networks combine to deliver a unique set of products and services that help people, businesses and governments realize their greatest potential.

www.mastercard.com

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.